PROYECTO DE TRABAJO DE GRADO

DEFINICIÓN DE UNA METODOLOGÍA PERSONALIZADA DE HACKING ÉTICO PARA EMPRESAS PÚBLICAS DE CUNDINAMARCA S.A. E.S.P Y EJECUCIÓN DE UNA PRUEBA A LA PÁGINA WEB Y A LOS SERVIDORES DE LA ENTIDAD, SOPORTADA SOBRE LA METODOLOGÍA DEFINIDA.

WILLIAM ANDRÉS SARMIENTO ACOSTA

ELKIN GERMAN RODRIGUEZ VASQUEZ

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C 15 JUNIO 2019

TABLA DE CONTENIDO

Introducción 13

1 Generalidades 16

1.1 Línea de Investigación 16

1.2 Planteamiento del Problema 16

1.2.1 Antecedentes del problema 17

1.2.2 Pregunta de investigación 18

1.3 Justificación 18

1.4 Objetivos 19

1.4.1 Objetivo general 19

1.4.2 Objetivos específicos 19

2 Marcos de referencia 20

2.1 Marco conceptual 20

2.2 Marco teórico 23

2.2.1 Guía Técnica PTES 23

2.2.2 Metodología OWASP 24

2.2.2.1 Top 10 OWASP. 27

2.2.2.2 Resumen deFactores de Riesgo del Top 10. 30

2.3 Marco jurídico 31

2.4 Marco geográfico 33

2.5 Estado del arte 34

3 Metodología del proyecto de grado 35

3.1 Fases del trabajo de grado 35

3.1.1 Fase de Planeación 35

3.1.2 Fase de Ejecución 35

3.1.3 Fase de Análisis 36

3.1.4 Fase de Informe 36

3.2 Instrumentos o herramientas utilizadas 37

3.2.1 Entrevista. 37

3.2.2 Herramientas utilizadas en la prueba técnica de la página Web. 37

3.2.2.1 Owasp Zap. 37

3.2.2.2 Nessus. 37

3.2.2.3 Acunetix. 37

3.2.2.4 Burpsuite. 38

3.2.2.5 Metasploit. 38

3.2.2.6 WPScan. 38

3.2.2.7 JoomScan. 39

3.2.2.8 Nikto. 39

3.2.3 Herramientas utilizadas en los Servidores 39

3.2.3.1 Nessus. 39

3.2.3.2 Nmap. 39

3.3 Población 40

3.4 Alcances y limitaciones 40

3.4.1 Alcance 40

3.4.2 Limitaciones 41

4 Productos a entregar 42

4.1 Clasificación de las Vulnerabilidades 42

4.1.1 Vulnerabilidad Crítica 43

4.1.2 Vulnerabilidad Alta. 43

4.1.3 Vulnerabilidad Media. 43

4.1.4 Vulnerabilidad Baja. 44

4.1.5 Vulnerabilidad Info. 44

4.2 metodología personalizada de ethical hacking para empresas públicas de Cundinamarca 44

4.3 aplicación de la metodología en las dos pruebas ejecutadas en empresas públicas 44

4.3.1 Interacciones Previas a la Prueba 45

4.3.1.1 Reunión de alcance. 45

4.3.1.2 Prueba de penetración de aplicaciones web. 46

4.3.1.3 Preguntas para los administradores de sistemas. 47

4.3.1.4 Reglas del compromiso 49

4.3.1.5 Establecer líneas de comunicación, los ejecutores de E.P.C. definirán los canales de comunicación para el desarrollo del proceso, estos pueden ser líneas telefónicas o celulares, correo electrónico u otro. 50

4.3.2 La recolección de información. 51

4.3.2.1 Herramientas utilizadas para la recopilación de información, el ejecutor debe suministrar una relación y detalle de las herramientas a utilizar para las pruebas. 51

4.3.2.2 Selección de objetivos 52

4.3.2.3 Huella. 54

4.3.3 Modelado de amenazas 55

4.3.3.1 Análisis de agentes o fuentes de amenazas / Análisis de la comunidad. 55

4.3.3.2 Modelado de Motivación de las Pruebas 56

4.3.3.3 Encontrar noticias relevantes de organizaciones comparables comprometidas. 57

4.3.4 Análisis e identificación de Vulnerabilidades 58

4.3.4.1 Pruebas de *Vulnerabilidad.* 58

4.3.4.2 Ejecución de escáneres de vulnerabilidades de red o sistemas. 58

4.3.4.3 Escáneres de aplicaciones web 59

4.3.4.4 Pruebas manuales / Protocolo específico 59

4.3.4.5 Investigación 60

4.3.4.6 Se realizará una explotación de bases de datos y frameworks. 60

4.3.4.7 Se evaluará la fortaleza de las contraseñas comunes y predeterminadas. 60

4.3.4.8 Se analizará la posibilidad de que existan debilidades de la configuración de aseguramiento. 61

4.3.5 Explotación 61

4.3.5.1 Propósito, el ejecutor y E.P.C. definirán el propósito del proceso de explotación controlada, que debe asociarse a la verificación de la existencia de vulnerabilidades y la prueba de eficacia de las medidas de protección existente. 61

4.3.5.2 Medidas de Protección, se verificarán la eficacia de las mismas. 61

4.3.5.3 Explotaciones a medida, se validará en consenso si se amerita la personalización de algún exploit como mecanismos de validación de una vulnerabilidad. 62

4.3.6 Post Explotación 62

4.3.6.1 Reglas de Compromiso 63

4.3.6.2 Análisis de infraestructura. 65

4.3.6.3 Servicios de red 66

4.3.6.4 Configuración del sistema. 66

4.3.6.5 Objetivos de alto valor / perfil 67

4.3.6.6 Limpieza 67

4.3.7 Informes 68

4.4 reconocimiento del objetivo web de e.p.c y resultados de las diferentes herramientas de escaneo web usadas 68

4.4.1 Nessus 69

4.4.2 Acunetix 69

4.4.3 OWASP ZAP 70

4.4.4 Nikto 71

4.4.5 Consolidación de las vulnerabilidades 71

4.4.6 Ataques a la aplicación web 76

4.4.7 WordPress 76

4.4.8 Joomla 79

4.4.9 Clickjacking 82

4.4.10 Indexación de Diccionarios 83

4.4.11 Cargue de archivos y suministros de credenciales de usuario en texto claro 84

4.5 reconocimiento del objetivo de infraestructura (servidores) de empresas publicas sa esp y resultados de las herramientas utilizadas. 87

4.6 modelo de seguridad y privacidad de la información – MSPI. 96

4.6.1 Análisis De Vulnerabilidades 97

4.7 entrega de resultados esperados e impactos 99

4.7.1 Aporte de los resultados a la Empresas Públicas de Cundinamarca 99

5 cómo se responde a la pregunta de investigación con los resultados 99

6 estrategias de comunicación y divulgación 100

7 Fortalezas y debilidades 100

7.1 Fortalezas 100

7.2 Debilidades 101

8 Conclusiones 102

9 Bibliografía 104

LISTA DE FIGURAS

ILUSTRACIÓN 1: EJECUCIÓN DE ATAQUE 25
ILUSTRACIÓN 2: CLASIFICACIÓN DE RIESGOS 26
ILUSTRACIÓN 3: RESUMEN CLASIFICACIÓN DE RIESGOS TOP 10 31
ILUSTRACIÓN 4: UBICACIÓN E.P.C 33
ILUSTRACIÓN 5: CLASIFICACIÓN RIESGO DE VULNERABILIDADES HALLADAS 42
ILUSTRACIÓN 6: WHOIS 54
ILUSTRACIÓN 7: PRIMERA NOTICIA RELACIONADA ATAQUES CIBERNETICOS 57
ILUSTRACIÓN 8: SEGUNDA NOTICIA RELACIONADA CIBERSEGURIDAD 57
ILUSTRACIÓN 9: RESULTADO DE ESCANEO NESSUS 69
ILUSTRACIÓN 10: RESULTADO ESCANEO ACUNETIX - VULNERABILIDADES 70
ILUSTRACIÓN 11: RESULTADO ESCANEO OWASP-ZAP 70
ILUSTRACIÓN 12:RESULTADO ESCANEO NIKTO 71
ILUSTRACIÓN 13: GRÁFICA TOTAL VULNERABILIDADES 76
ILUSTRACIÓN 14: ESCANEO GESTOR DE CONTENIDO WORDPRESS 77
ILUSTRACIÓN 15: FUERZA BRUTA CON BURPSUITE A WWW.EPC.COM.CO 78
ILUSTRACIÓN 16: ESCANEO CON WPSCAN A WWW.EPC.COM.CO 79
ILUSTRACIÓN 17: ESCANEO GESTOR DE CONTENIDO JOOMLA 80
ILUSTRACIÓN 18: ATAQUE DESDE EL METASPLOIT AL JOOMLA 81
ILUSTRACIÓN 19: SESIÓN DE METERPETER CERRADA - JOOMLA 81
ILUSTRACIÓN 20: PRUEBA ONLINE DE UN ATAQUE CLICKJACKING 82
ILUSTRACIÓN 21: LISTADO DIRECTORIO VIA WEB 83
ILUSTRACIÓN 22: INFORMACIÓN EN TEXTO CLARO 85
ILUSTRACIÓN 23: VERIFICACION DEL CERTIFICADO DIGITAL DE EPC 86
ILUSTRACIÓN 24: SERVIDORES PRINCIPALES FÍSICOS 87
ILUSTRACIÓN 25: SERVIDOR HUÉSPED VIRTUALIZADO 87
ILUSTRACIÓN 26: PRIMER SERVIDOR NAS 88
ILUSTRACIÓN 27: SEGUNDO SERVIDOR NAS 88
ILUSTRACIÓN 28: TERCER SERVIDOR NAS 88
ILUSTRACIÓN 29: CONFIGURACIÓN DE RED EN EL EQUIPO 88
ILUSTRACIÓN 30: INICIO DE NESSUS EN KALI LINUX 89
ILUSTRACIÓN 31: TIPO DE ESCANEO SELECCIONADO EN NESSUS 89
ILUSTRACIÓN 32: CONFIGURACIÓN PARA CADA ESCANEO 90

ILUSTRACIÓN 33: ESCANEO SERVIDOR HUÉSPED Y ANFITRIÓN 90
ILUSTRACIÓN 34: ESCANEO SEGUNDO SERVIDOR FÍSICO 91
ILUSTRACIÓN 35: PRIMER SERVIDOR NAS 91
ILUSTRACIÓN 36: SEGUNDO SERVIDOR NAS 92
ILUSTRACIÓN 37: TERCER SERVIDOR NAS 92
ILUSTRACIÓN 38: IDENTIFICACIÓN DE EQUIPO DE CONTABILIDAD 93
ILUSTRACIÓN 39: ESCANEO EQUIPO EN RED DE CONTABILIDAD USADO COMO REPOSITORIO 93
ILUSTRACIÓN 40: MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 97

LISTA DE TABLAS

TABLA 1: LEYES Y DECRETOS....33
TABLA 2: VULNERABILIDAD CLICKJACKING....73
TABLA 3: VULNERABILIDAD ACCESO DIRECTORIOS VÍA WEB....73
TABLA 4: VULNERABILIDAD DE JOOMLA....74
TABLA 5: AUTOCOMPLETADO DE CONTRASEÑAS....74
TABLA 6: VULNERABILIDAD CSRF....74
TABLA 7:VULNERABILIDAD CARGUE DE ARCHIVOS....75
TABLA 8: VULNERABILIDAD CERTIFICADO DIGITAL....75
TABLA 9: VULNERABILIDAD INFO....75
TABLA 10: VULNERABILIDADES HALLADAS EN EL ESCANEO SERVIDORES....96

INTRODUCCIÓN

Empresas Públicas de Cundinamarca S.A. E.S.P., es una empresa constituida el 19 de mayo del 2008, de carácter oficial, con autonomía administrativa, patrimonial y presupuestal, cuyo principal accionista es la **GOBERNACIÓN DE CUNDINAMARCA**, que tiene como objeto principal prestar servicios públicos domiciliarios de acueducto, alcantarillado, aseo, energía y gas, entre otros; así como servicios públicos no domiciliarios y el desarrollo de actividades complementarias inherentes a los mismos. (E.P.C., 2018)

En concordancia con su objeto social y como Gestora del Plan Departamental para el Manejo Empresarial de los Servicios de Agua y Saneamiento PAP-PDA, impulsa estrategias que permiten avanzar con celeridad en la cobertura urbana y rural de los servicios de acueducto y saneamiento básico, así como las transformaciones para el manejo empresarial de los mismos. Su gestión está orientada al mejoramiento de la calidad de vida de los cundinamarqueses, teniendo como referencia planes, programas y políticas del orden nacional, departamental y municipal que se encuentran en desarrollo. (E.P.C., 2018)

Las entidades del sector público han venido implementando a través del Ministerio de las Tecnologías MINTIC planes, programas y lineamientos que les permita establecer políticas que fortalezcan los aspectos de seguridad de la información en sus diferentes procesos de manejo de información, sin embargo no están exentas a sufrir incidentes de seguridad sobre la información más cuando día a día se están reinventando las formas de vulnerar las infraestructuras tecnológicas de las empresas, independientemente sean multinacionales o pymes, los atacantes buscan descubrir los activos de estas y proceder con ataques de acuerdo con las vulnerabilidades encontradas y así

poder obtener beneficios, ya sean de índole económica, o solamente por tener la satisfacción del logro de acceso a la información de las empresas.

Los focos de ataque en su mayoría son el usuario final, ya que después de realizar un reconocimiento por parte del atacante (ingeniería Social) los usarios, al no poseer un conocimiento claro de qué hacer o no hacer en temas de seguridad, pueden dar acceso inconscientemente a los atacantes. *De acuerdo con cifras dadas por la compañía Digiware, diariamente, en Colombia (2017) se producen en promedio 542.465 ataques informáticos, las redes criminales realizan hurtos a diario que superan los $100 millones en Colombia a través del correo electrónico. Así se distribuyen los ataques por sectores económicos:* (Revista Dinero, 2017)

- El sector financiero: 214.600 ataques por día (39,56%).
- Telecomunicaciones: 138.329 ataques por día (25,5%).
- El sector Gobierno: 83.756 ataques por día (15,44%)
- Sector energético: 19.583 ataques por día (3,61%)
- Industria: 51.263 ataques por día (9,45%).
- Retail: 34.934 (6,44%) (Revista Dinero, 2017)

Teniendo en cuenta lo anterior, lo que se busca realizar en el trabajo de grado es un procesos de Ethical Hacking, en donde se pueda evaluar el estado de seguridad de los sistemas de información de Empresas Públicas de Cundinamarca, con el fin de encontrar vulnerabilidades e identificar las fallas que se estén presentando por falta de control y aseguramiento de la

información crítica de la compañía. La idea del proyecto es dar a conocer a la empresa el estado actual de sus servidores de información y como la compañía debe remediar estas brechas de seguridad y emitir sugerencias de cómo mejorar la seguridad de sus activos, esto se consignará en un informe para la Gerencia y el área de TI de la compañía en donde se explique lo mencionado anteriormente.

El interés y motivación de realizar el proyecto anteriormente mencionado es el de aplicar cada uno de los conceptos adquiridos durante el plan de estudios de la especialización, es de gran valor tener la oportunidad ampliar los conocimientos en Hacking Ético y poder aplicarlos de forma eficaz. Por lo cual, el proyecto se basará en metodologías y guías técnicas ya establecidas para el escaneo y análisis de vulnerabilidades a nivel de red y a nivel de aplicación, como lo son la PAUTAS TÉCNICAS PTES y OWASP TOP 10.

1 GENERALIDADES

1.1 LÍNEA DE INVESTIGACIÓN

El proyecto se enmarca en la línea de investigación Software inteligente y convergencia tecnológica, ya que permitirá realizar pruebas de penetración a la infraestructura de Empresas Públicas de Cundinamarca S.A. E.S.P, posterior a esto se hará un análisis de las vulnerabilidades encontradas y se podrá entregar a la empresa un informe detallado de cómo debe remediar las vulnerabilidades en base a las buenas prácticas para mantener una infraestructura segura.

1.2 PLANTEAMIENTO DEL PROBLEMA

Preservar la confidencialidad, disponibilidad e integridad de la información (ICONTEC, 2006), es una prioridad para cualquier entidad u organización, sin embargo, en el SECTOR PÚBLICO este tipo de medidas y políticas se han venido implementando de manera paulatina y en algunas organizaciones de forma más lenta, por lo cual, existen falencias que pueden llegar a afectar significativamente el nivel de Seguridad en los procesos que ejecutan a diario los diferentes sistemas de Información.

En el contexto de la seguridad y en términos del estándar ISO 27001, un riesgo puede ser expresado como el efecto de la incertidumbre sobre los objetivos de seguridad de la información. También, están asociados a la causa potencial de que una amenaza pueda explotar una o más vulnerabilidades de un activo o grupo de activos de información, teniendo como consecuencia algún tipo de impacto.(Miguel Ángel Mendoza, 2015)

Generalmente, los riesgos se expresan en términos de la combinación de la posibilidad de ocurrencia de un evento no deseado (probabilidad) y sus consecuencias (impacto), por lo que las medidas de seguridad están orientadas a reducir alguna de estas dos variables, o en el mejor de los casos a ambas. (Miguel Ángel Mendoza, 2015)

El informe anual de Symantec (ISTR), que analiza 157 países, reveló que en 2017 Colombia fue el sexto país de Latinoamérica con el mayor número de ataques cibernéticos detectados. De acuerdo con el informe, Colombia sufrió el 0.36% de todas las amenazas que se reportaron en América Latina durante el 2017, siendo los Bots y el Spam las estrategias más comunes. (COLPRENSA, 2018)

1.2.1 Antecedentes del problema

El problema de Empresas Públicas de Cundinamarca es que aun siendo la entidad descentralizada más grande de la GOBERNACIÓN DE CUNDINAMARCA, no cuenta con un área de tecnología ni un área de seguridad de la información conformada dentro de su organigrama que le brinde un respaldo constante, eficiente y oportuno en cuanto a la gestión tecnológica y el aseguramiento de la información que esta maneja, el recurso humano a cargo es temporal lo cual hace que no se tenga un ingeniero base con los conocimientos sólidos en todo lo relacionado con la gestión de TI y seguridad en los sistemas de información que maneja la entidad, desconociendo las vulnerabilidades o incidentes que pueden llegar en su momento a afectar el normal funcionamiento de los sistemas de información instalados en sus servidores, así como la pérdida parcial o total de información almacenada en los mismos, o dicho de otra forma, desconociendo amenazas y debilidades que de materializarse afectasen la disponibilidad, integridad y

confidencialidad de la información y lo sistemas de información de la entidad.

Empresas Publicas de Cundinamarca S.A ESP es una entidad en formación pues hace 8 años que fue constituida y continúa actualmente en un proceso constante de mejora en todos sus componentes administrativos y funcionales, en la actualidad no se tiene evidencia de la realización de pruebas de seguridad informática de alguna índole que le permita a la entidad determinar en qué condiciones se encuentra en lo que respecta a las normas y estándares aplicables a la seguridad de la información. Los procesos en el área de tecnología están dirigidos a fortalecer los sistemas de información, algunos de los cuales aún se encuentran en desarrollo, así como garantizar el almacenamiento y disponibilidad permanente de la información que manejan los funcionarios y contratistas.

1.2.2 Pregunta de investigación

¿Puede una prueba de ethical hacking identificar potenciales amenazas, vulnerabilidades y riesgos de la infraestructura tecnológica de Empresas Públicas de Cundinamarca, particularmente de los servidores y la página web, que permita la toma de medidas de mitigación y prevención?

1.3 JUSTIFICACIÓN

Las estadísticas en Colombia nos muestran que es un país vulnerable, en el cual los incidentes de seguridad cada vez son más frecuentes en el sector público o privado y la probabilidad de que Empresas Públicas de Cundinamarca pueda ser víctima es considerable si no mantiene unos lineamientos, protocolos y buenas prácticas de seguridad bien establecidos.

Con la ejecución de la prueba de Hacking Ético en Empresas Públicas, se le permitirá a la

entidad determinar qué tan segura se encuentra su página web y la información alojada en sus servidores, así como generar de manera oportuna estrategias para fortalecer la seguridad de la información y la potencial remediación de un incidente de seguridad que se pueda presentar en un momento determinado.

De igual forma es vital para la entidad el cumplimiento de los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) en su Estrategia de Gobierno en línea (GEL), que corresponden al componente de Continuidad del Negocio y Gestión de Incidentes en las entidades del estado del orden territorial.

Este plan de Respuesta sobre Incidentes de Seguridad de la Información estará alineado con el ciclo de vida de Respuesta a Incidentes de Seguridad (Preparación, Detección y Análisis, Contención – Erradicación – Recuperación Y Actividades Post-Incidente) definido por MINTIC, señalado en el Modelo de Seguridad y Privacidad de la Información, Guía 21 Gestión de Incidentes. (CCP-MINTIC, 2016)

1.4 OBJETIVOS

1.4.1 Objetivo general

- Diseñar una metodología de hacking ético que permita la ejecución de una primera prueba a la página web y los servidores de empresas públicas de Cundinamarca S.A ESP.

1.4.2 Objetivos específicos

- Construir a partir de metodologías de evaluación de seguridad existentes, una metodología

propia para aplicar en la entidad.

- Ejecutar un Pentesting Test a la página web de entidad aplicando la metodología definida.

- Ejecutar un Pentesting Test a los servidores de la entidad aplicando la metodología definida.

- Generar un informe gerencial, técnico y de recomendaciones de las pruebas realizadas a partir de la metodología construida.

2 MARCOS DE REFERENCIA

2.1 MARCO CONCEPTUAL

A continuación, se describirán las palabras claves pertenecientes al entorno de seguridad de la información e informática que serán expresadas en el contexto del proyecto de grado.

- **Confidencialidad:** Propiedad que permite que la información esté disponible o sea revelada a personas, entidades o procesos autorizados.

- **Integridad:** Propiedad de la exactitud y no la alteración de la información por partes no autorizadas.

- **Disponibilidad:** Propiedad de la información para estar accesible y utilizable al ser solicitada por una entidad autorizada.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (Alfonso Lorenzo Perez, 2019)

- **Amenaza:** Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio. (MINTIC,s.f)

- **Vulnerabilidad:** Una vulnerabilidad es un estado de debilidad en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad de los sistemas. (MINTIC,s.f)

- **Caja Blanca:** En el caso de contar con información previa detallada de la organización.

- **Caja Gris:** En el caso de contar con información parcial de la organización.

- **Caja Negra**: Aquellas auditorías que se realizan sin información previa por parte de la organización.

- **Ethical Hacking:** Es una serie de pruebas o test denominados “Test de penetración” cuyo objetivo es poder burlar las diferentes vallas de seguridad que tiene la red para diferentes

organizaciones, con la única intención de probar su efectividad, o por el contrario, demostrar la vulnerabilidad de aquel sistema.

- **Análisis de Vulnerabilidades:** Por medio de herramientas especializadas en análisis de vulnerabilidades, se realiza un análisis a los dispositivos del cliente con el fin de identificar los riesgos sobre las aplicaciones y servicios que soportan estas. (Iniseg, 2018)

- **Penetration Test:** Una prueba de penetración consiste en pruebas ofensivas contra los mecanismos de defensa existentes en el entorno que se está analizando. Estas pruebas comprenden desde el análisis de dispositivos físicos y digitales, hasta el análisis del factor humano utilizando Ingeniería Social. (Fernando Catoira, 2012)

- Red Team: Prueba de intrusión o hacking ético intrusivo que utiliza la terminología militar para referirse al equipo atacante ético como los que simulan ser los delincuentes, este tipo de actividad es más elaborada y profunda que un análisis de vulnerabilidades o una prueba de penetración y se componen de campañas que agrupan un número de ataques particulares normalmente ya materializados en empresas del mismo gremio que el cliente. En contexto también existe el Blue Team y se refiere al equipo que se encarga de proteger a la organización de los ataques del Red Team y los reales atacantes y ciberdelincuentes.

2.2 MARCO TEÓRICO

2.2.1 Guía Técnica PTES

El estándar de ejecución de pruebas de penetración, en inglés Penetration Testing Execution Estándar (PTES), consta de siete (7) secciones principales. Estos cubren todo lo relacionado con una prueba de penetración, desde la comunicación inicial y el razonamiento detrás de un pentest, a través de la recopilación de inteligencia y las fases de modelado de amenazas donde los evaluadores trabajan detrás de escena para obtener una mejor comprensión de la organización a evaluar, a través de la investigación de vulnerabilidad. Explotación y post explotación, donde la experiencia en seguridad técnica de los evaluadores viene a jugar y se combina con la comprensión comercial del compromiso y, finalmente, con el informe, que captura todo el proceso, de una manera que tiene sentido para el cliente y proporciona más valor para él. (GNU Free Documentation, 2014)

Esta versión puede considerarse una versión 1.0, ya que los elementos centrales de la norma se han solidificado y los autores la han "probado en la trayectoria" durante más de un año a través de la industria. Próximamente los autores estarán trabajando en una versión 2.0 que proporcionará un trabajo más granular en términos de "niveles", como en los niveles de intensidad en los que se puede realizar cada uno de los elementos de una prueba de penetración. Como ningún pentest es como otro, y las pruebas variarán desde la aplicación web más mundana o la prueba de red, hasta el compromiso de una prueba total por el “Red Team”, dichos niveles permitirán a la organización definir cuánta sofisticación esperan que muestren sus adversarios, y posibilitar al evaluador donde debe aumentar la intensidad de aquellas áreas en que la organización más las necesita o es débil.

(GNU Free Documentation, 2014)

Las siguientes son las principales secciones definidas por el estándar como la base para la ejecución de las pruebas de penetración:

- Interacciones previas al compromiso
- Recolección de información
- Modelado de amenazas
- Análisis de vulnerabilidad
- Explotación
- Post explotación
- Informes (GNU Free Documentation, 2014)

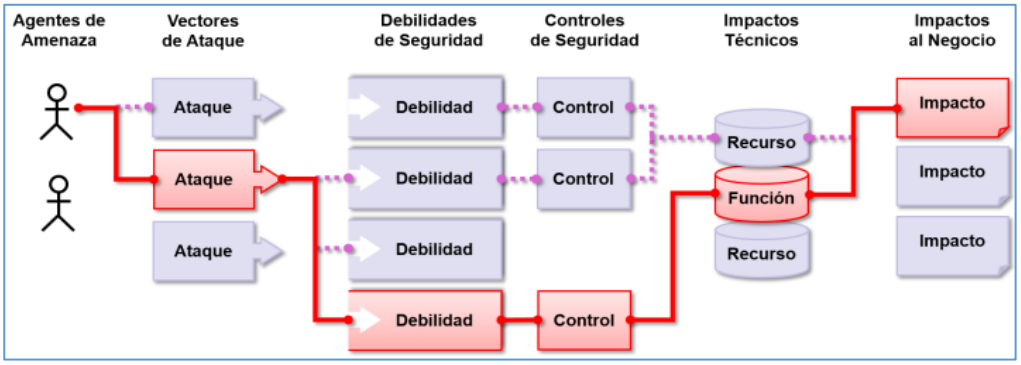
2.2.2 Metodología OWASP

El OWASP Top 10 -2017, se trata del top de debilidades de aplicaciones web, es decir el ranking de debilidades de aplicaciones web que está ocurriendo con mayor frecuencia en internet se basa principalmente en él envió de datos de más de 40 empresas que se especializan en seguridad de aplicaciones y una encuesta de la industria que fue completada por más de 500 personas. Esta información abarca vulnerabilidades recopiladas de cientos de organizaciones y más de 100.000 aplicaciones y APIs del mundo real. Las 10 principales categorías fueron seleccionadas y priorizadas de acuerdo con estos datos de prevalencia, en combinación con estimaciones consensuadas de explotabilidad, detectabilidad e impacto. (OWASP Foundation, 2017, p4)

Uno de los principales objetivos de OWASP Top 10 es educar a los desarrolladores, diseñadores, arquitectos, gerentes y organizaciones sobre las consecuencias de las debilidades más comunes y más importantes de la seguridad de las aplicaciones web. El Top 10 proporciona técnicas básicas para protegerse contra estas áreas con problemas de riego alto, y proporciona orientación sobre cómo continuar desde allí. (OWASP Foundation, 2017, p4)

Los atacantes pueden, potencialmente, utilizar diferentes rutas (Ilustración 1) a través de su aplicación para perjudicar su negocio u organización. Cada uno de estos caminos representa un riesgo que puede o no ser suficientemente grave como para merecer atención.(OWASP Foundation, 2017, p6)

Ilustración 1: Ejecución de Ataque



Fuente: (OWASP Foundation, 2017, p6)

Algunas veces, estos caminos son fáciles de encontrar y explotar, mientras que otras son extremadamente difíciles. De la misma manera, el perjuicio ocasionado puede no tener consecuencias, o puede dejarlo en la quiebra. A fin de determinar el riesgo para su organización, puede evaluar la probabilidad asociada a cada agente de amenaza, vector de ataque, debilidad de

seguridad y combinarlo con una estimación del impacto técnico y de negocio para su organización. Juntos, estos factores determinan su riesgo general. (OWASP Foundation, 2017, p6)

El OWASP Top 10 se enfoca en identificar los riesgos más críticos para un amplio tipo de organizaciones. Para cada uno de estos riesgos, se proporciona información genérica sobre la probabilidad y el impacto técnico, utilizando el siguiente esquema de evaluación, basado en la Metodología de Evaluación de Riesgos de OWASP. (OWASP Foundation, 2017, p6)

Ilustración 2: Clasificación de Riesgos

Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

Fuente: (OWASP Foundation, 2017, p6)

Cada organización es única, y también lo son los agentes de amenaza para esa organización, sus objetivos y el impacto de cualquier brecha. Si una organización de interés público utiliza un sistema de gestión de contenido (CMS) para manipular información pública y el sistema de salud utiliza el mismo CMS para tratar datos sensibles, los agentes de amenaza y los impactos en el negocio son muy distintos para el mismo software. Es fundamental comprender el riesgo para su organización en función de los agentes de amenaza aplicables a su negocio y los impactos comerciales. (OWASP Foundation, 2017, p6)

En la medida de lo posible, los nombres de los riesgos en el Top 10 están alineados con el

marco de las debilidades del CWE, Common Weakness Enumeration de Mitre (organismo estadounidense sin ánimo de lucro que gestiona centros de investigación y desarrollo para un mundo seguro) , se trata de lineamientos que promueven el lenguaje comun para la medición, identificación, mitigación y prevención de debilidades de seguridad en el software, de estar forma se promueven prácticas de seguridad generalmente aceptadas y se reduce la confusión. (OWASP Foundation, 2017, p6)

2.2.2.1 Top 10 OWASP.

A continuación, se explica en detalle el TOP 10 del OWASP del año 2017:

- **A1:2017 Inyección**

Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete o intermediario, como parte de un comando o consulta a una base de información en background. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización. (OWASP Foundation, 2017, p7)

- **A2:2017 Pérdida de Autenticación**

Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros

usuarios (temporal o permanentemente). (OWASP Foundation, 2017, p7)

- **A3:2017 Exposición de datos sensibles**

Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito. (OWASP Foundation, 2017, p7)

- **A4:2017 Entidades Externas XML (XXE)**

Muchos procesos XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS). (OWASP Foundation, 2017, p7)

- **A5:2017 Pérdida de Control de Acceso**

Las restricciones sobre lo que los usuarios autenticados pueden hacer en muchas ocasiones no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc. (OWASP Foundation, 2017, p7)

- **A6:2017 Configuración de Seguridad Incorrecta**

La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, ad hoc (improvisada) o por omisión (o directamente por la falta de configuración). Son ejemplos: S3 buckets abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, frameworks, dependencias y componentes desactualizados, etc.

- **A7:2017 Secuencia de Comandos en Sitios Cruzados (XSS)**

Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecutara JavaScript en el navegador de los siguientes usuarios. Permite ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar (defacement) los sitios web, o redireccionar al usuario hacia un sitio malicioso. (OWASP Foundation, 2017, p7)

- **A8:2017 Deserialización Insegura**

Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor. (OWASP Foundation, 2017, p7)

- **A9:2017 Componentes con vulnerabilidades conocidas**

Los componentes como bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos. (OWASP Foundation, 2017, p7)

- **A10:2017 Registro y Monitoreo Insuficientes**

El registró (logs de trazabilidad y auditoria) y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos. (OWASP Foundation, 2017, p7)

2.2.2.2 Resumen deFactores de Riesgo del Top 10.

La siguiente tabla presenta un resumen del Top 10 y los factores de riesgo que hemos asignado a cada uno de ellos. Estos factores fueron determinados basándose en las estadísticas disponibles y la experiencia del equipo del OWASP Top 10. Para entender estos riesgos en una aplicación en particular u organización, usted debe considerar sus propias fuentes o agentes de amenaza e impactos específicos del negocio. Incluso las vulnerabilidades graves de software podrían no representar un riesgo serio si no hay agentes de amenaza en posición para ejecutar el ataque necesario, o el impacto al negocio es insignificante para los activos involucrados. (OWASP Foundation, 2017, p23)

Ilustración 3: Resumen Clasificación de Riesgos Top 10

Riesgo	Agentes de Amenaza	Vectores de Ataque	Debilidades de Seguridad		Impacto		Puntuación
		Explotabilidad	Prevalencia	Detectabilidad	Técnico	Negocio	
A1: 2017- Inyección	Específico de la Aplicación	FACIL: 3	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	8,0
A2: 2017 - Pérdida de Autenticación	Específico de la Aplicación	FACIL: 3	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0
A3: 2017 - Exposición de Datos Sensibles	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0
A4: 2017 - Entidad Externa de XML (XXE)	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	7,0
A5: 2017 - Pérdida de Control de Acceso	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	6,0
A6: 2017 - Configuración de Seguridad Incorrecta	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0
A7: 2017 - Secuencia de Comandos en Sitios Cruzados (XSS)	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0
A8: 2017 - Deserialización Insegura	Específico de la Aplicación	DIFICIL: 1	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	5,0
A9: 2017 - Componentes con Vulnerabilidades Conocidas	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	MODERADO: 2	Específico de la Aplicación	4,7
A10: 2017 - Registro y Monitoreo Insuficientes	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	DIFICIL: 1	MODERADO: 2	Específico de la Aplicación	4,0

Fuente: (OWASP Foundation, 2017, p23)

2.3 MARCO JURÍDICO

TIPO	AÑO	DESCRIPCIÓN
Ley 1712	2014	Transparencia y del Derecho a la Información Pública. (Congreso de la República de Colombia, 2014)
Decreto 1151	2007	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962

		de 2005, y se dictan otras disposiciones. (Ministerio de la Comunicaciones, 2014)
Ley 1273	2009	"por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". (Senado de la República de Colombia, 2009)
Ley 1581	2012	Por el cual se dictan disposiciones generales para la protección de datos personales. (Senado de la República de Colombia, 2012)
Ley 527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. (Congreso de la República de Colombia, 1999)

Ley 1266	2008	Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. (Congreso de la República de Colombia, 2008)

Tabla 1: Leyes y Decretos

2.4 MARCO GEOGRÁFICO

El proyecto se desarrollará en las oficinas de Empresas Públicas de Cundinamarca S.A ESP ubicadas en Avenida Calle 24 No 51-40 Piso 11, Bogotá - Colombia.

Ilustración 4: Ubicación E.P.C

Fuente: Google Maps

2.5 ESTADO DEL ARTE

Camilo Alfonso Guzmán Flórez, Cristian Andrés Angarita Pinzón, Proyecto (Protocolos para la mitigación de ciberataques en el hogar. Casos de estudio: Estratos 3 y 4 de la ciudad de Bogotá). El protocolo de mitigación de ciberataques se consolida como una herramienta útil, en primer lugar, para dar a conocer los riesgos más comunes y en segundo lugar para culturizarla la gente del común de cómo enfrentarse a ellos y lograr reducirlos o mitigarlos. Además, la divulgación de este tipo de herramientas cumple con el objetivo de generar cambio de cultura mediante la modificación de conductas inseguras. (Angarita Pinzón & Guzmán Flórez, 2017)

Miguel Andres Meneses Ortiz, Anderson Julián Llanos Ruiz, Proyecto (Diseño de un protocolo de vulnerabilidades en los principales servidores de la superintendencia de puertos y transportes) El trabajo pretende realizar un análisis de vulnerabilidades que pueden contener los servidores de la Superintendencia de Puertos y Transportes, corregirlas y diseñar un protocolo que oriente cómo se debe actuar en casos futuros cuando se encuentren nuevas vulnerabilidades, con el fin de garantizar el óptimo funcionamiento de los equipos y permitir la disponibilidad de la información en todo momento.(Llanos Ruiz & Meneses Ortiz, 2016)

Allen David Zuluaga Mateus, Proyecto (Hacking Ético basado en la metodología abierta de testeo de seguridad – OSSTMM, aplicado a la Rama Judicial, Seccional Armenia). La realización del presente hacking ético genera un impacto positivo en las políticas de seguridad de la información, pues se constituye en un elemento de entrada que permite la toma de decisiones basadas en hechos, en pro de la seguridad de la información. Esto a su vez redunda en un beneficio

para los usuarios del aparato judicial, pues la información asociada a sus procesos judiciales se encontrará mejor protegida, generando una mayor confianza. (Zuluaga Mateus, 2017)

3 METODOLOGÍA DEL PROYECTO DE GRADO

3.1 FASES DEL TRABAJO DE GRADO

Para el desarrollo de nuestro proyecto de grado se define las siguientes fases:

3.1.1 Fase de Planeación

En esta fase buscamos las organizaciones en las cuales cada uno de quienes participamos en la realización de este proyecto trabajamos con el fin de reunirnos con los directivos y exponerles el proyecto académico.

3.1.2 Fase de Ejecución

En esta fase presentamos la propuesta formal de trabajo a Empresas Publicas y nos reunimos primero con el área directiva para exponerles el proyecto, posteriormente nos reunimos con los ingenieros del área de tecnología socializarles el plan de trabajo propuesto y acordar la forma en la cual realizaríamos las pruebas técnicas y así mismo especificarles los protocolos de seguridad que debían tener previstos para garantizar que en dado caso que se presentara algún tipo de falla tuviéramos lo necesario para restablecer los servicios de forma oportuna y sin poner en riesgo la operación de la organización.

3.1.3 Fase de Análisis

En esta fase se realiza una reunión técnica con el área de tecnología que nos permita tener una visual de la infraestructura física que tiene la entidad, sus servicios web y su centro de procesamiento de datos. Bajo este primer contexto determinar las herramientas que se usarían en la realización de las pruebas técnicas y las condiciones adecuadas de ejecución que no interfirieran en el normal funcionamiento de los procesos de la entidad.

De igual forma en esta fase se procede a hacer un análisis de la metodología PTES que nos permita a partir de esta generar una nueva metodología personalizada para la ejecución de un ethical hacking en Empresas Publicas de Cundinamarca.

3.1.4 Fase de Informe

En esta fase final se procede a realizar la elaboración de los informes técnicos y gerenciales a partir de los resultados obtenidos en las pruebas técnicas realizadas previamente que serán socializados en Empresas Publicas y serán soporte como entregables del proyecto.

Se realiza el respectivo diseño de la metodología personalizada para Empresas Públicas de Cundinamarca.

3.2 INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

3.2.1 Entrevista.

Se realiza una reunión con los ingenieros del área de sistemas de E.P.C, con el fin de que nos suministren información respecto los servidores y la página web, así mismo, que nos comenten con qué frecuencia se realiza la actualización de los servidores y si se han presentado (si aplica) algún ataque informático.

3.2.2 Herramientas utilizadas en la prueba técnica de la página Web.

3.2.2.1 Owasp Zap.

Es un escáner de seguridad web de código abierto. Pretende ser utilizado como una aplicación de seguridad y como una herramienta profesional para pruebas de penetración. (OWASP-ZAP, 2019)

3.2.2.2 Nessus.

Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un proceso residente en memoria, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.(Wikipedia, 2017)

3.2.2.3 Acunetix.

Acunetix es una herramienta automatizada de prueba de seguridad de aplicaciones web que audita sus aplicaciones web al verificar vulnerabilidades como Inyección de SQL, secuencias de

comandos entre sitios y otras vulnerabilidades explotables. En general, Acunetix escanea cualquier sitio web o aplicación web que sea accesible a través de un navegador web y use el protocolo HTTP / HTTPS. (Acunetix, s.f.)

3.2.2.4 Burpsuite.

Es una herramienta gráfica para probar la seguridad de las aplicaciones web, fue desarrollado para proporcionar una solución integral para verificaciones de seguridad de aplicaciones web. Además de la funcionalidad básica, como el servidor proxy, el escáner y el intruso, la herramienta también contiene opciones más avanzadas, araña, repetidor, decodificador, comparador, extensor y un secuenciador. (Wikipedia, 2019)

3.2.2.5 Metasploit.

Es un proyecto de seguridad informática que proporciona información sobre vulnerabilidades de seguridad y ayuda en las pruebas de penetración y el desarrollo de firmas IDS. Su subproyecto más conocido es el Metasploit Framework de código abierto [2], una herramienta para desarrollar y ejecutar código de explotación contra una máquina de destino remota. (Wikipedia, 2019)

3.2.2.6 WPScan.

Es un escáner de vulnerabilidad de WordPress de caja negra gratuito, para uso no comercial. Al utilizar el WPScan, se puede comprobar si un sitio de WordPress contiene vulnerabilidades conocidas en los archivos cores, plugins y temas. (Alycia Mitchell, 2015)

3.2.2.7 JoomScan.

Es un proyecto de código abierto en lenguaje de programación Perl para detectar las vulnerabilidades web de Joomla CMS y analizarlas.(OWASP Joomla, 2018)

3.2.2.8 Nikto.

Es un escáner de vulnerabilidad de línea de comandos de software gratuito que escanea los servidores web en busca de archivos / CGI peligrosos, software de servidor obsoleto y otros problemas. Realiza verificaciones genéricas y específicas del tipo de servidor. También captura e imprime las cookies recibidas. El código Nikto en sí mismo es software libre. (Wikipedia, 2019)

3.2.3 Herramientas utilizadas en los Servidores

3.2.3.1 Nessus.

Es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un proceso residente en memoria, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.(Wikipedia, 2017)

3.2.3.2 Nmap.

Nmap ("Network Mapper") es una herramienta gratuita de código abierto para la exploración de la red o la auditoría de seguridad. Fue diseñado para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales. Nmap utiliza paquetes IP para determinar qué hosts están disponibles en la red, qué servicios (nombre de la aplicación y la

versión) estos equipos ofrecen, qué sistemas operativos (y versiones del sistema operativo) se están ejecutando, qué tipo de filtros de paquetes o cortafuegos están en uso, y docenas de otras características.(EUGENIO DUARTE, 2012)

Las herramientas anteriormente descritas fueron ejecutadas desde máquinas virtuales (VirtualBox) específicamente desde el sistema operativo Kali Linux con sus actualizaciones más recientes.

3.3 POBLACIÓN

Las pruebas aplicadas en Empresas Publicas se realizaron sobre el dominio principal donde se aloja la página web de la entidad, siendo esta la única publicación web de la entidad y sobre la totalidad de los servidores internos, siendo estos los dos principales y los tres de almacenamiento en red.

3.4 ALCANCES Y LIMITACIONES

3.4.1 Alcance

Realizar una única prueba de hacking ético sobre la página web y los servidores de Empresas Públicas de Cundinamarca S.A ESP, con el fin de detectar falencias de seguridad que puedan exponer la confidencialidad, integridad y disponibilidad de la información que estos manejan en sus diferentes procesos administrativos, de tal forma que nos permita entregar un documento detallado con los resultados encontrados, donde se especifique cada prueba realizada y evidencie las vulnerabilidades existentes, sugiriendo a la entidad las medidas preventivas y/o

correctivas que deba tomar para mejorar la seguridad sus servidores y página web.

3.4.2 Limitaciones

Teniendo como referencia lo sensible de la información alojada en los servidores de la entidad y que en estos se encuentran instalados sistemas de información importantes para sus operaciones financieras y de proyectos, la ejecución de este tipo de pruebas puede llegar a ocasionar inconvenientes en la disponibilidad de los servicios, no será una prueba técnica intrusiva y en todo momento se estará controlando las actividades con los responsables de la entidad para evitar que de alguna forma altere la confidencialidad, integridad y disponibilidad de la información y los sistemas de información.

Limitante en cuanto a la publicación del trabajo por confidencialidad de la información en cuanto a los resultados obtenidos.

La ejecución de las pruebas sobre los servidores se debe programar de tal forma que no genere ningún tipo de interrupción de los procesos administrativos que se soportan en los sistemas de información instalados en el mismo.

Los escaneos se deben realizar en horarios acordados con los ingenieros de la entidad según su disponibilidad.

4 PRODUCTOS A ENTREGAR

La realización de un proceso de Ethical Hacking en una empresa le permite determinar su nivel de seguridad informática y le puede llevarla a alcanzar un nivel de protección óptimo, esto con el fin salvaguardar de forma adecuada la información alojada dentro y fuera de su infraestructura, es así como posterior a la ejecución de la prueba técnica sobre los servidores de la entidad y su dominio, los productos a entregar serán:

- Diseño de metodología personalizada para ejecución de pruebas
- Informe técnico de la página web.
- Informe técnico servidores de la entidad.
- Recomendaciones y/o buenas prácticas para mejorar la seguridad en la entidad.
- Informe gerencial.

4.1 CLASIFICACIÓN DE LAS VULNERABILIDADES

A continuación, se muestra la tabla en donde se dará la clasificación de los riesgos por cada una de las vulnerabilidades halladas en el servidor interno o la página web.

Clasificación Riesgo de Vulnerabilidades			
Alta	Media	Baja	Info

Ilustración 5: *Clasificación Riesgo de Vulnerabilidades Halladas*

4.1.1 Vulnerabilidad Crítica

Este tipo de vulnerabilidad permite la propagación de amenazas sin que sea necesaria la participación del usuario, también se tratan de vulnerabilidades cuyos métodos de aprovechamiento son ampliamente conocidos y su impacto es muy alto o catastrófico

4.1.2 Vulnerabilidad Alta.

Este tipo de vulnerabilidad es capaz de poner en riesgo la confidencialidad, integridad o disponibilidad de los datos de los usuarios y/o la organización, como así también, la integridad o disponibilidad de los recursos de procesamiento que este disponga. De igual forma se tratan de vulnerabilidades con métodos de aprovechamiento ampliamente conocidos

4.1.3 Vulnerabilidad Media.

Este es uno de los tipos de vulnerabilidades más sencillas de combatir, ya que el riesgo que presenta se puede disminuir con medidas tales como configuraciones predeterminadas, auditorías y demás. Aparte, las vulnerabilidades medias no son aprovechadas en todo su potencial ya que no afecta a un gran número de usuarios. Complementariamente se tratan de vulnerabilidades cuyo mecanismo de aprovechamiento no son ampliamente conocidos o son complejos y dada su potencial materialización tendría un impacto medio para la organización.

4.1.4 Vulnerabilidad Baja.

Este tipo de vulnerabilidad es realmente muy difícil de aprovechar por un atacante, y su impacto es mínimo, ya que no afecta a una gran masa de usuarios.

4.1.5 Vulnerabilidad Info.

Este tipo de vulnerabilidad es realmente de información respecto al escaneo que se realice, su impacto es mínimo, sin embargo, puede dar información validación para complementar las vulnerabilidades con riesgos más altos.

4.2 METODOLOGÍA PERSONALIZADA DE ETHICAL HACKING PARA EMPRESAS PÚBLICAS DE CUNDINAMARCA

El modelo de metodología personalizada (basada en el estándar de ejecución de pruebas de penetración - PTES) con sus respectivas fases para la entidad se evidencia como **anexo 1** de este documento.

4.3 APLICACIÓN DE LA METODOLOGÍA EN LAS DOS PRUEBAS EJECUTADAS EN EMPRESAS PÚBLICAS

Esta metodología plantea la ejecución de unas pruebas de hacking ético de tipo pruebas de intrusión o penetración testing de caja blanca, esto quiere decir que se tratan de pruebas que además de buscar la existencia de vulnerabilidades intentaran de forma controlada la explotación como confirmación de la existencia de las mismas, todo esto suministrando la información básica necesaria para que lo ejecutores conozcan el contexto técnico y aceleren el proceso de ejecución.

4.3.1 Interacciones Previas a la Prueba

Etapa inicial en la cual se define los diferentes aspectos que se van a realizar en las diferentes pruebas, así como los tiempos y días de ejecución. En esta fase se han de hablar y acordar por escrito los diversos aspectos de la prueba de penetración.

4.3.1.1 Reunión de alcance.

Se realizó una reunión inicial la cual nos permitió exponer ante la dirección encargada de tecnología que en este caso es la Secretaria de Asuntos Corporativos lo que pretendíamos realizar con las pruebas de ethical hacking y los beneficios que la entidad podría llegar a obtener.

En una reunión posterior presentamos ante la dirección encargada y los ingenieros de tecnología de EPC SA ESP nuestro plan de trabajo el cual contemplaba las fases en las que se iba a desarrollar las pruebas de Ethical Hacking:

- Definición de metodología personalizada, aplicable a la entidad.
- Pruebas de Ethical Hacking a la página web de la entidad
- Pruebas de Ethical Hacking a los servidores que alojan información y/o aplicaciones de la entidad.

Se hace claridad que se realizará una única prueba para cada caso y que en ningún momento se ejecutaran pruebas intrusivas que vulneren la seguridad e inestabilicen el normal funcionamiento de los sistemas de información.

4.3.1.2 Prueba de penetración de aplicaciones web.

Se realiza la prueba de penetración sobre el dominio principal sobre el cual está la página web de la entidad que corresponde a: www.epc.com.co

- ¿Cuántas aplicaciones web están siendo evaluadas?

  Solamente se evalúa el dominio principal de la entidad.

- Indique cuales son las direcciones IP y los URLs de las aplicaciones a evaluar.
  - URL: www.epc.com.co
  - IP 192.232.249.14
- ¿Cuál es la tecnología de construcción de cada una de las aplicaciones?

  La página web comparte dos gestores de contenidos, WordPress y Joomla.

- ¿Cuántas aplicaciones web de las que están evaluando tienen inicio de sesión, de tal forma que contemplen usuario y roles de operación?, de existir alguna, ¿suministre credenciales (usuario y contraseña) de un usuario de bajo perfil con que el que se pueda probar si existe alguna potencial vulnerabilidad de escalamiento de privilegios?

  No fueron suministrados los usuarios para estas pruebas.

4.3.1.3 Preguntas para los administradores de sistemas.

Las siguientes preguntas fueron realizadas a los ingenieros de tecnología de la entidad con el fin de tener claridad de los sistemas de información que actualmente tienen en funcionamiento y sobre los cuales se basan sus actividades principales.

- ¿Hay algún sistema que pueda caracterizarse como frágil?

Los sistemas de información con los que actualmente cuenta la entidad están en un proceso constante de mejora y perfeccionamiento. Los procesos de soporte técnico y actualización están supeditado a vínculos contractuales con terceros.

- ¿Cuáles son los servidores objetivos de la prueba?, de igual forma indique cuál es su sistema operativo.

  La entidad solo permite describir que son servidores de información.

- ¿Cuáles sistemas de información se alojan en los servidores objetivos de la prueba?

  Por acuerdo de confidencialidad con la entidad esta información no podrá ser descrita en este documento.

- Indique cuales son los rangos de las direcciones IP de la organización y ¿cuáles son las direcciones IP de los servidores objetivo de la prueba?

La entidad solo suministra las IP de los servidores a escanear, por acuerdo de confidencialidad con la entidad esta información no podrá ser descrita en este documento.

- ¿Hay sistemas en la red que no sean propiedad y/o administración de E.P.C que puedan requerir de una aprobación adicional?

Se tiene sistemas de información los cuales no están alojados directamente en los servidores de la entidad, sino que para su uso los usuarios se conectan a servidores en la nube o físicos de otra organización como los son el sistema para la gestión de proyectos AQUACUN y el sistema de gestión de correspondencia MERCURIO.

- ¿Cuál es el tiempo medio para reparar las interrupciones de los sistemas?

Los tiempos de respuesta por fallas en los sistemas están supeditados a los tiempos de respuesta que los proveedores de los mismos establezcan en sus contratos de soporte y mantenimiento.

- ¿Existe algún software de monitoreo de los sistemas de información?

No se tiene para los diferentes sistemas de información ningún software de monitoreo o seguimiento.

- ¿Cuáles son los servidores y aplicaciones más críticos?

El servidor principal en el cual se aloja el sistema de información (no se suministra más

información por acuerdo de confidencialidad con la entidad) es el de mayor importancia para la entidad.

- ¿Las copias de seguridad son probadas regularmente?

Se realizan copias de seguridad programadas todos los días sobre los sistemas de información, pero no se tiene un entorno de prueba en el cual en algún momento las copias de seguridad se hayan comprobado para validar que se estén realizando de forma correcta.

- ¿Cuándo fue la última vez que se restauraron las copias de seguridad?

No se ha requerido realizar restauraciones de copias de seguridad para los sistemas de información respaldados en el último año.

4.3.1.4 Reglas del compromiso

Se da claridad a los ingenieros de tecnología de qué forma se van a autorizar los procedimientos y el tratamiento de los resultados arrojados en cada prueba realizada.

- Manejo de evidencia, los ejecutores de la prueba y E.P.C acordaran el manejo de la información, tanto operacionalmente como a nivel de confidencialidad de la información.

Los resultados obtenidos de las pruebas realizadas serán únicamente usados para los análisis que permitan dar un concepto final del estado en el cual la entidad está en temas de

seguridad, que tan vulnerable seria ante un ataque y hasta qué punto podría verse afectado. Estos resultados nunca serán conocidos por terceros hasta que la entidad no aplique los correctivos que garanticen la solución de estas, de tal forma que no se vulnere la privacidad de la información o se ponga en riesgo la seguridad de los sistemas.

- Permiso para realizar las pruebas, E.P.C. debe aprobar algún documento que evidencie la autorización de la ejecución de las pruebas.

Previa realización de cada prueba se les comunica a los ingenieros de tecnología de la entidad de tal forma que se realicen los protocolos de seguridad que permita validar los respaldos que sean necesarios en el sistema, así como el acompañamiento del proceso para evitar inconvenientes en la ejecución.

4.3.1.5 Establecer líneas de comunicación, los ejecutores de E.P.C. definirán los canales de comunicación para el desarrollo del proceso, estos pueden ser líneas telefónicas o celulares, correo electrónico u otro.

Las líneas de comunicación oficial serán únicamente por correo electrónico oficial tanto de los estudiantes como de los ingenieros de tecnología de entidad, con el propósito de validar las reuniones o confirmar las pruebas a realizar en las fechas previamente definidas. Por ninguna circunstancia se usará el correo para enviar información producto de los análisis realizados ni ningún tipo de esta que esté catalogada por la entidad como confidencial y/o sensible.

4.3.2 La recolección de información.

En esta etapa se hace la recopilación de toda la información respecto a las pruebas realizadas sobre el objetivo. En esta fase del pentest se busca obtener toda la información posible de la organización que se encuentre disponible de tal forma que nos permita hacernos una idea de los sistemas y funcionamiento.

4.3.2.1 Herramientas utilizadas para la recopilación de información, el ejecutor debe suministrar una relación y detalle de las herramientas a utilizar para las pruebas.

Las herramientas que se usaron para hacer un levantamiento previo de la información y conocer más el contexto de funcionamiento y entorno de ejecución sobre el cual la organización realiza sus procesos fue:

- Entrevista nivel directivo: Se realizó una reunión con la directora encargada del área que permitiera exponer de manera general lo que se pretende realizar y conocer diferentes aspectos en el funcionamiento del área de tecnología en la organización.

- Entrevista nivel técnico: se realizó una reunión con los ingenieros de tecnología para conocer la infraestructura que soporte la organización, ubicación de los servidores, características, estructura de red y sistemas de información que dispone la entidad para sus procesos.

4.3.2.2 Selección de objetivos

Se deja claridad a la organización sobre qué parte de la infraestructura se van a ejecutar las pruebas, puntualizando en cada uno de los objetivos.

- Identificación y nombre del objetivo

  - Página web: www.epc.com.co
  - Servidores de aplicación
  - Servidores NAS

- Considerar las limitaciones de las reglas de compromiso.

A continuación, son presentadas una serie de consideraciones que deben ser tenidas en cuenta por ambas partes antes de dar inicio a la PRUEBAS TÉCNICAS DE ETHICAL HACKING:

Es necesario y responsabilidad de EMPRESAS PÚBLICAS DE CUNDINAMARCA SA ESP brindar el acompañamiento, los permisos y las autorizaciones requeridas para la realización de cada uno de los ítems que contiene la metodología.

Se recomienda a EMPRESAS PÚBLICAS DE CUNDINAMARCA SA ESP tener copias de respaldo de los datos y las configuraciones de los sistemas y dispositivos incluidos dentro del alcance del proyecto, previa ejecución del ejercicio. Y de igual forma las pruebas se realizarán en

una ventana de mantenimiento que minimice la afectación de los servicios ante un probable reinicio de los mismos.

Si se encuentran vulnerabilidades y estas puedan ser explotadas por los estudiantes para saber qué información sensible pueda ser hallada, los estudiantes notificarán a EMPRESAS PÚBLICAS DE CUNDINAMARCA SA ESP, con el fin de que estos autoricen expresamente la ejecución de las pruebas de explotación ya sea sobre el servidor interno o la página web.

- Considerar la duración del tiempo aproximado para la ejecución de cada prueba.

La duración de las pruebas se enmarca en periodos de tiempo que pueden oscilar de 2 a 4 horas donde no estén en un rango crítico en la jornada laboral. Las pruebas que en su duración puedan ser superiores a 4 horas deben ser realizadas de forma remota en días no hábiles o jornada nocturna.

- Considerar el objetivo final de la prueba

Los objetivos de cada prueba realizada con las diferentes herramientas será evidenciar las vulnerabilidades que puedan tener la página web de la entidad o los servidores de aplicación y almacenamiento de información. De tal forma que nos permita dar un concepto final sobre el estado de la seguridad en la organización y qué acciones son recomendables implementar para mejorar

4.3.2.3 Huella.

- Huella externa
  - Reconocimiento pasivo
  - Se realiza la búsqueda en internet (WHOIS) a quien está asociado el dominio epc.com.co.

Ilustración 6: WHOIS

Información de dominio

Dominio:	epc.com.co
Registrador:	Central Comercializadora de Internet SAS
Registrado en:	2008-10-20
Expira el:	2019-10-19
Actualizado en:	2018-10-03
Estado:	Transferencia cliente Prohibido
Servidores de nombres:	ns2185.hostgator.com ns2186.hostgator.com

Contacto del Registrante

Organización:	EMPRESAS PUBLICA DE CUNDINAMARCA SA ESP-9002223460
Estado:	Distrito Capltalde Santa Fede Bogotá & # 227;
País:	CO

Fuente: https://www.whois.com/whois/epc.com.co

- Huella activa
  - Reconocimiento Activo
  - Escaneo de puertos
  - Escaneo de Usuarios
  - Identificación de sistemas operativos

- Rangos de IP

4.3.3 Modelado de amenazas

Se analiza el contexto, las herramientas a utilizar y la infraestructura sobre la cual se van a realizar los ataques de la forma más eficiente y óptima. Definimos nuestra estrategia de penetración, respecto a los objetivos identificados.

4.3.3.1 Análisis de agentes o fuentes de amenazas / Análisis de la comunidad.

Definir las comunidades y los agentes de amenaza relevantes, se debe proporcionar una identificación clara.

- Análisis del recurso humano interno
  - **Funcionarios:** Personas que tiene un vínculo laboral permanente con la entidad a través de un contrato laboral.
  - **Contratistas**: Personas con vinculación temporal con la entidad, según la necesidad.
  - **Ingenieros de Tecnología**: personas contratistas que brindan el soporte de toda la infraestructura de la entidad y los sistemas de información.
  - **Conexiones remotas:** Conexiones realizadas por empleados de la entidad para

realizar actividades laborales con aplicaciones no confiables.

- Análisis del recurso humano externos
    - **Proveedores**: Quienes tiene a cargo el soporte técnico y mantenimiento de los diferentes sistemas de información sobre los cuales trabaja la entidad.

    - **Demás empresas competidoras**: Entidades del sector público que realicen actividades similares a la de Empresas de Servicios Públicos de Cundinamarca.

    - **Piratas informáticos:** Personas motivadas para obtener información sensible y distribuirla sin consentimiento para fines lucrativos.

- Análisis de herramientas en uso.

Software que puedan llegar a ser instalado por parte de los empleados de forma no autorizada en los equipos de la entidad.

4.3.3.2 Modelado de Motivación de las Pruebas

La posible motivación de los agentes / comunidades de amenaza para realizar la afectación en los sistemas de la entidad, por el tipo de organización pública gubernamental puede ser:

- Reconocimiento, beneficio particular, saboteo, interrupción de los servicios, dines económicos.

4.3.3.3 Encontrar noticias relevantes de organizaciones comparables comprometidas.

Ilustración 7: Primera Noticia Relacionada Ataques Ciberneticos

Fuente: (Revista Dinero, 2018)

Ilustración 8: Segunda Noticia Relacionada Ciberseguridad

Fuente: (El Tiempo, 2017)

4.3.4 Análisis e identificación de Vulnerabilidades

En esta fase se realiza una identificación proactiva de vulnerabilidades con los datos recogidos previamente, se determina las vías de ataque y métodos a utilizar, conocidos como FingerPrinting (Scanning y Enumeración). Se define el ámbito y alcance del test de intrusión con el fin de alcanzar los objetivos previamente definidos.

4.3.4.1 Pruebas de *Vulnerabilidad.*

Proceso que permite descubrir fallas la página web de la entidad o los servidores de la entidad las cuales pueden ser aprovechadas por un atacante. Estas fallas pueden variar desde la configuración incorrecta del host y el servicio. Aunque el proceso utilizado para buscar fallas varía y depende en gran medida del componente en particular que se está probando, algunos principios clave se aplican al proceso.

4.3.4.2 Ejecución de escáneres de vulnerabilidades de red o sistemas.

Exploración automatizada basada en puertos para determinar lo que está disponible en la red o el host objetivo.

Para el escaneo de los servidores web se utilizan herramientas actualizadas open source o que son de uso permitido a nivel educativo como Nessus, Nmap, las cuales nos darán a conocer las vulnerabilidades encontradas con el fin de dar a conocer a la empresa como corregirlas.

4.3.4.3 Escáneres de aplicaciones web

- Se ejecutarán escáneres de identificación de debilidades en aplicaciones web.

Para el escaneo de la página web www.epc.com.co se utilizan herramientas actualizadas open source o que son de uso permitido a nivel educativo como Nessus, Owasp Zap, Nikto, Acunetix los cuales nos ayudarán a encontrar vulnerabilidades de la página las cuales se procede a analizar y dar un diagnóstico para que a su vez la empresa corrija estos posibles huecos de seguridad.

- Se identificarán las versiones del servidor web, administrador de contenido y componentes, para luego investigar si estos presentan alguna vulnerabilidad identificación de vulnerabilidad.

El servidor web es nginx/1.14.1, en el cual tiene configurados dos gestores de contenido, un Joomla versión 1.5.15 de 2009 y un WordPress versión 4.5.17 de 2019

4.3.4.4 Pruebas manuales / Protocolo específico

- Se realizarán pruebas manuales para la explotación, confirmación y potencial explotación controlada.

De acuerdo a las vulnerabilidades encontradas se hará o no la prueba de penetración de forma manual o mediante las herramientas de explotación del Kali Linux

4.3.4.5 Investigación

- Investigación pública (identificación del problema), se realizará una investigación de las vulnerabilidades encontradas, su forma de aprovechamiento, la existencia de exploits y los posibles compromisos e impactos que pueden tener.

    - Bases de datos de vulnerabilidad (verificar un problema notificado por una herramienta o para revisar manualmente la vulnerabilidad)

    - Avisos de seguridad emitidos por proveedores

4.3.4.6 Se realizará una explotación de bases de datos y frameworks.

No se presenta vulnerabilidad de con el fin de llegar a tener acceso a la base de datos.

4.3.4.7 Se evaluará la fortaleza de las contraseñas comunes y predeterminadas.

Después de lo encontrado por el escaneo, se realiza un ataque de fuerza bruta, ya que existen gestores de contenido, y a uno de estos se pudo enumerar los usuarios administradores, por lo cual se pueden validar la fortaleza de las contraseñas.

4.3.4.8 Se analizará la posibilidad de que existan debilidades de la configuración de aseguramiento.

La información de aseguramiento o la validación de errores comunes se tomará de la base de datos de vulnerabilidades como la CVE, CWE - MITRE y NVD, que nos darán datos claros de cuál es el riesgo de dicha vulnerabilidad y como se debe remediar la misma.

4.3.5 Explotación

En esta fase de acuerdo a las herramientas que hemos seleccionado procedemos a realizar los ataques respectivos para buscar explotar las vulnerabilidades previamente identificadas. Identificamos y definimos vectores de ataque.

4.3.5.1 Propósito, el ejecutor y E.P.C. definirán el propósito del proceso de explotación controlada, que debe asociarse a la verificación de la existencia de vulnerabilidades y la prueba de eficacia de las medidas de protección existente.

El objetivo principal es identificar el punto de entrada en la página web o servidores de la organización e identificar los activos objetivos de alto valor que pueda llegar a verse afectados en su confidencialidad, integridad y/o disponibilidad.

4.3.5.2 Medidas de Protección, se verificarán la eficacia de las mismas.

Son tecnología preventiva o controles que implementa la entidad como medida de

protección y las cuales dificultan la capacidad de completar con éxito el proceso de explotación.

- Antivirus: Todos los equipos de la entidad cuentan con un antivirus corporativo debidamente licenciado por el proveedor del servicio.

- Firewall: La compañía cuenta con firewall, pero no es de última generación.

- Firewall de aplicaciones web (WAF): El servidor web cuenta con la protección de un WAF, ya que en las pruebas realizadas de penetración al gestor de contenido Joomla de la página donde se aprovecha una vulnerabilidad, este cierra la conexión remota.

4.3.5.3 Explotaciones a medida, se validará en consenso si se amerita la personalización de algún exploit como mecanismos de validación de una vulnerabilidad.

- Personalización de exploits

No se realiza personalización de exploits, solo para una prueba en una vulnerabilidad se ejecuta un exploit ya encontrado dentro de la base de datos del Framework Metasploit

4.3.6 Post Explotación

En esta etapa se pretende tener acceso a los sistemas de forma permanente de tal forma que podamos evidenciar hasta donde tenemos control y acceso y a la información. Presentación de

reportes (ejecutivo y técnico) como conclusión de lo realizado. En esta fase tratamos de conseguir el máximo nivel de privilegios, información de la red y acceso al mayor número posible de sistemas identificando datos y/o servicios, así como sus niveles de importancia.

4.3.6.1 Reglas de Compromiso

Se específicas las consideraciones necesarias para que en esta fase de la prueba se garantice en todo momento que los sistemas de la entidad estén expuestos lo menos posible a riesgos innecesarios por las acciones (directas o indirectas) de las ejecuciones realizadas.

Los procedimientos previos estarán soportados en un plan de trabajo realizado para la entidad y el cual debe ser firmado por los ingenieros de tecnología en el cual se especifica los tipos de pruebas a realizar, así como las recomendaciones que se deben tener en todo momento con los sistemas de información, servidores y pagina web.

- Proteger al cliente

Previo a la realización de las pruebas para la página web y los servidores de la entidad se tuvieron las siguientes consideraciones que permitieran garantizar la calidad de la prueba y que los datos no estén expuestos a riesgos:

  - Cualquier modificación realizada en los cambios de configuración se informó previamente a los ingenieros de tecnología de la entidad.

- Se documentó de forma detallada cada una de las acciones ejecutadas contra la página web o servidores.

- En ningún momento se utilizarán servicios de terceros para descifrar contraseñas o realizar algún tipo de procedimiento.

- Los registros con acciones y tiempos registrados durante la evaluación se guardaron, procesarán y se plasmaron en los respectivos informes técnicos y gerenciales producido.

- En ninguno de las pruebas realizadas se eliminó, borrar o modificar algún tipo registros.

❖ Protegiéndose

Antes de la ejecución de la prueba se aseguró que los ingenieros de tecnología respaldaran de forma correcta todas las bases de datos. Dejando por escrito desde un inicio en el plan de trabajo las responsabilidades de la entidad y de los estudiantes de la universidad católica de Colombia, en aspectos como:

- Se hizo claridad a los ingenieros de tecnología respecto a las pruebas que se van a realizar.

- Se validaron previa realización de cada prueba que no se tuvieran fallos evidentes en la página web o servidor que pudieran después comprometer la calidad en la ejecución de la prueba.

- Se hicieron las recomendaciones al área de tecnología con el fin de tomar las medidas preventivas necesarias y que minimizará una posible afectación generada en la en la ejecución de la prueba en cuanto al normal funcionamiento de los sistemas e información alojada en los servidores, así como la página web.

4.3.6.2 Análisis de infraestructura.

❖ Configuración de red

Se realizó un escaneo de red con una herramienta automatizada que permitió identificar las direcciones IP las cuales están asignadas a los servidores de la entidad que son las siguientes:

- Servidores Principal
- Servidor Virtualizado
- Servidores NAS de almacenamiento en red

  Nota: Por acuerdo de confidencialidad con la entidad esta información no podrá ser descrita en este documento.

4.3.6.3 Servicios de red

- Servidores de bases de datos

Se identificó que el sistema principal de la entidad está alojado en un servidor anfitrión de virtualización el cual tiene un motor de base de datos SQL Server.

- Virtualización

El servidor virtualizado huésped que tiene la entidad en su dirección IP interna la cual por acuerdo de confidencialidad con la entidad no podrá ser descrita en este documento.

- Sistemas de respaldo

La entidad no tiene ninguna aplicación que automatice el proceso de copias de respaldo, están programadas directamente en el gestor de base de datos y almacenadas en el disco duro del servidor físico en el cual se encuentra virtualizado el sistema administrativo y financiero.

4.3.6.4 Configuración del sistema.

- Política de contraseñas

En su política de seguridad la entidad establece que las diferentes contraseñas que se manejan para los sistemas de información y demás aplicativos deben cumplir una longitud de

mínimo 8 caracteres alfanuméricos, minúsculas, mayúsculas y ser actualizadas cada cierto periodo de tiempo por lo funcionarios.

4.3.6.5 Objetivos de alto valor / perfil

Los objetivos de alto valor que se pudieron identificar en las pruebas realizadas son los siguientes:

- Base de datos del sistema de información de la entidad.
- Información de los funcionarios almacenada en los servidores NAS.
- Credenciales de inicio de sesión para los usuarios creados en los gestores de contenido.

4.3.6.6 Limpieza

Una vez finalizadas las diferentes pruebas a los dos objetivos identificados se procedió en cada caso a eliminar cualquier archivo o configuración realizada de forma temporal:

- Eliminación de todos los archivos ejecutables, scripts y temporales de un sistema comprometido.
- Restaurar los valores originales del sistema y a los parámetros de configuración de

la aplicación.

- Eliminar todas las puertas traseras y / o rootkits instalados.

4.3.7 Informes

En esta etapa final se procese a realizar la documentación que nos permita dar un concepto objetivo sobre el estado de seguridad de la organización, posterior a los análisis realizados a cada uno de los resultados obtenidos en las diferentes etapas. En los informes generados se debe independizar la parte técnica de la parte gerencial, detallando siempre los puntos en los que la seguridad se había implantado de manera correcta y aquellos en los que debe haber demorado y la forma más eficiente de hacerlo.

- Informe de estado de seguridad de los servidores.
- Informe de estado de seguridad en la página web.
- Informe gerencial.

4.4 RECONOCIMIENTO DEL OBJETIVO WEB DE E.P.C Y RESULTADOS DE LAS DIFERENTES HERRAMIENTAS DE ESCANEO WEB USADAS

Consiste en el uso de diversos programas de escaneo y pruebas web, para luego realizar la comparación de cada uno de los resultados arrojados por estos, con el fin de evitar falsos positivos, permitiendo garantizar que las vulnerabilidades encontradas pueden generar algún riesgo para la organización, el dominio a analizar es www.epc.com.co.

Las herramientas ejecutadas fueron:

4.4.1 Nessus

Al realizar la ejecución de la herramienta Nessus con la plantilla de Web Application Scanning, la cual nos arroja las vulnerabilidades del sitio web, la herramienta cataloga los hallazgos de la siguiente manera, 8 con riesgo medio y 118 tipos Info

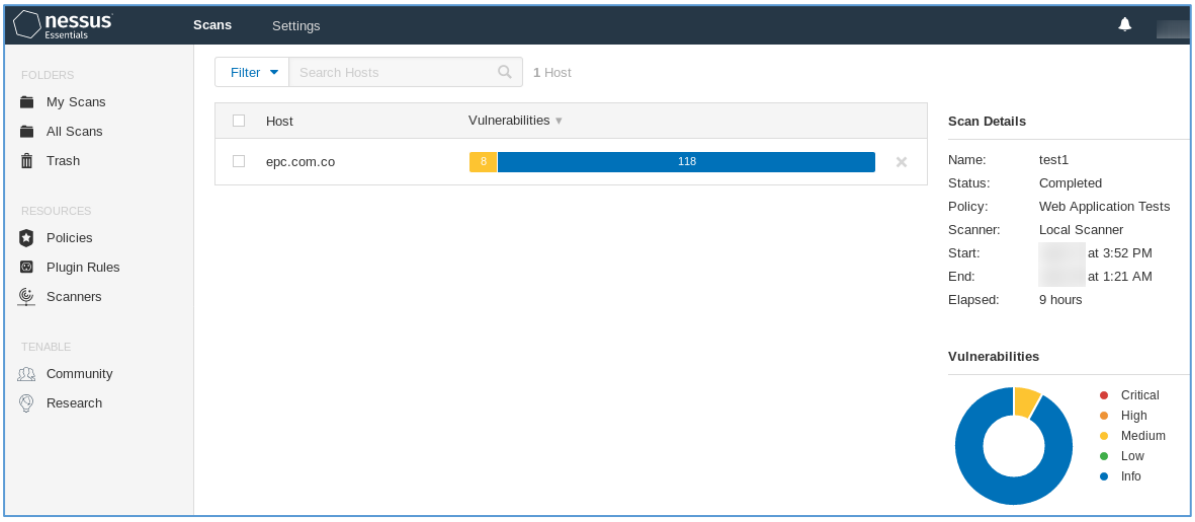


Ilustración 9: Resultado de Escaneo Nessus

4.4.2 Acunetix

Con la ejecución del programa Acunetix, Se pusieron encontrar varias vulnerabilidades del dominio www.epc.com.co como se evidencia en la imagen a continuación:

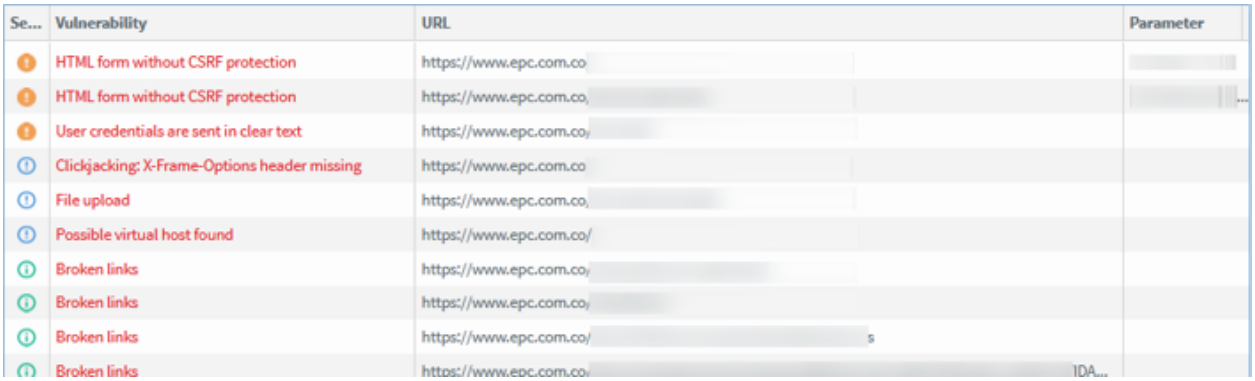


Ilustración 10: Resultado Escaneo Acunetix - Vulnerabilidades

4.4.3 OWASP ZAP

Esta herramienta del proyecto OWASP ZAP, que se encuentra en la distribución Kali Linux, se ejecutó con el fin de detectar las vulnerabilidades a nivel web, los hallazgos se componen de 1 vulnerabilidad con riesgo medio y 8 con riesgo bajo.

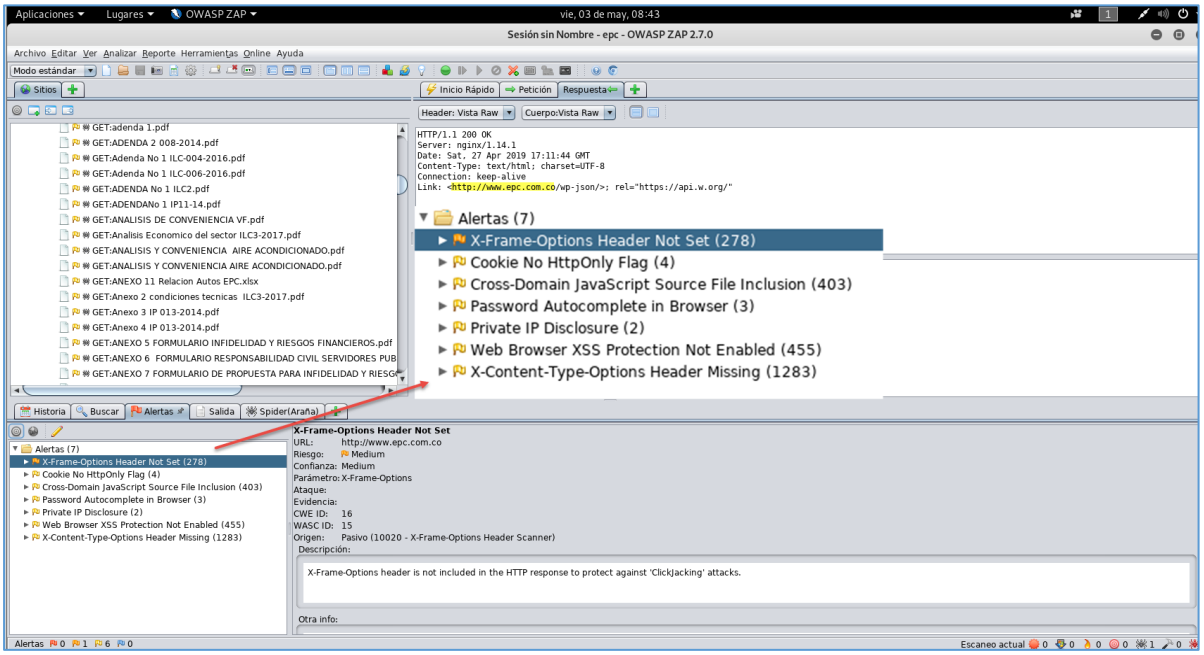


Ilustración 11: Resultado Escaneo Owasp-Zap

4.4.4 Nikto

Esta es otra herramienta ejecutada desde Kali Linux, que permite realizar un escaneo de vulnerabilidades web, este escaneo de forma complementaria nos permite evidenciar vulnerabilidades que las herramientas anteriormente descritas no mostraron y se deben tener en cuenta en el análisis o ponderación de vulnerabilidades con el fin de evitar los falsos positivos.

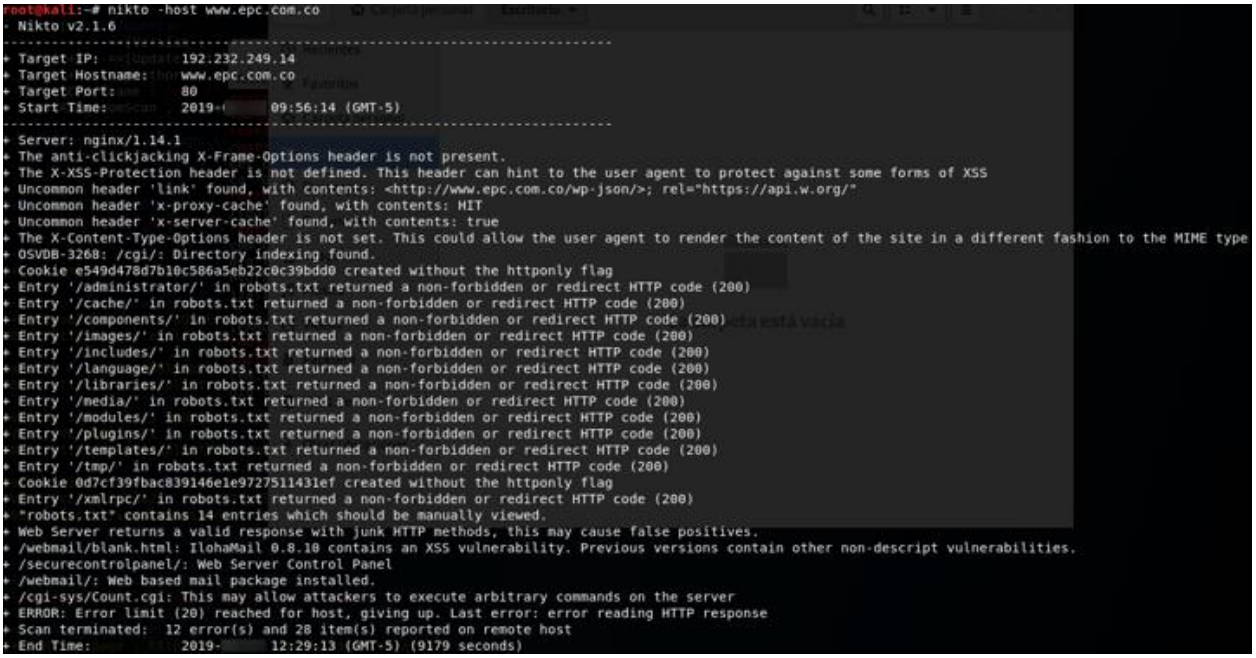


Ilustración 12:Resultado Escaneo Nikto

4.4.5 Consolidación de las vulnerabilidades

Respecto a los datos de las herramientas usadas para el escaneo web al dominio www.epc.com.co .

Herramienta	Vulnerabilidad	Factor de Riesgo	Riesgo Propuesto	Descripción
Nessus	Web Application Potentially Vulnerable to Clickjacking	Medio	Medio	Clickjacking, también conocido como "ataque de reparación de la interfaz de usuario", es cuando un atacante usa varias capas transparentes u opacas para engañar a un usuario para que haga clic en un botón o enlace en otra página cuando intentaba hacer clic en la página de nivel superior. Por lo tanto, el atacante está "secuestrando" los clics destinados a su página y enrutándolos a otra página, probablemente propiedad de otra aplicación, dominio o ambos.
Owasp-zap	X-Frame-Options Header Not Set	Medio	Medio	
Acunetix	Clickjacking:X-Frame-Options header missing	Bajo	Medio	

Nitko	The anti-clickjacking X-Frame-Options header is not present	Info	Medio	

Tabla 2: *Vulnerabilidad Clickjacking*

Herramienta	Vulnerabilidad	Factor de Riesgo	Riesgo Propuesto	Descripción
Nessus	Browsable Web Directories	Medio	Medio	Tiene directorios indexados que pueden ser fácilmente accedidos por los usuarios desde la web, por ejemplo, acceso al archivo robots.txt o /cgi/
Nitko	Evidencia de Directorios	Info	Medio	

Tabla 3: *Vulnerabilidad Acceso Directorios vía Web*

Herramienta	Vulnerabilidad	Factor de Riesgo	Riesgo Propuesto	Descripción
Nessus	Joomla! Detection	Medio	Alto	Dicha vulnerabilidad se encuentra en el filtrado inadecuado de la información del "user agent" al guardar los valores de la sesión en la base de datos, lo que podría permitir la ejecución de código arbitrario. Se le ha asignado el CVE-2015-8562. Es vulnerabilidad afecta a las versiones 1.5 hasta la 3.4.5 y que utilicen PHP igual o inferior a la versión 5.4.45.
Owasp-zap	Directorio /Administrator	Bajo	Alto	

Acunetix	Directorio /Administrator	Bajo	Alto	
Nitko	Directorio /Administrator	Info	Alto	

Tabla 4: Vulnerabilidad de Joomla

Herramienta	Vulnerabilidad	Facto de Riesgo	Riesgo Propuesto	Descripción
Owasp-zap	Password Autocomplete in Browser	Bajo	Bajo	El atributo AUTOCOMPLETE no está deshabilitado en un elemento HTML FORM / INPUT que contiene una entrada de tipo de Password. Las contraseñas pueden almacenarse en los navegadores y recuperarse.

Tabla 5: Autocompletado de Contraseñas

Herramienta	Vulnerabilidad	Facto de Riesgo	Riesgo Propuesto	Descripción
Acunetix	HTML form without CSRF protection	Medio	Medio	Este ataque fuerza al navegador web de su víctima, validado en algún servicio (como por ejemplo correo o home banking) a enviar una petición a una aplicación web vulnerable.

Tabla 6: Vulnerabilidad CSRF

Herramienta	Vulnerabilidad	Factor de Riesgo	Riesgo Propuesto	Descripción
Acunetix	File Upload	Bajo	Bajo	Si los archivos cargados no se verifican de manera segura, un atacante puede cargar archivos maliciosos.

Tabla 7:Vulnerabilidad Cargue de Archivos

Herramienta	Vulnerabilidad	Factor de Riesgo	Riesgo Propuesto	Descripción
Acunetix	User credentials are sent in clear text	Bajo	Bajo	Un tercero puede leer las credenciales del usuario interceptando una conexión HTTP sin cifrar.

Tabla 8: Vulnerabilidad Certificado Digital

Herramienta	Vulnerabilidad	Factor Riesgo	Riesgo Propuesto	Descripción
Acunetix	Broken Links	Info	Informativo	Información a la cual no se tiene acceso o no se puede visualizar, validación de toda la información alojada en el servidor, con el fin de clasificar lo que se puede mostrar al público y lo que no.
Nessus	Broken Links	Info	Infamativo	

Tabla 9: Vulnerabilidad Info

En general, en relación al número total de amenazas encontradas mediante el escaneo de la página principal www.epc.com.co , cabe resaltar que las vulnerabilidades catalogadas como Informativas fueron alrededor de 118, sin embargo, realizando una ponderación entre los resultados arrojados por cada una de las herramientas de escaneo se observa que se trata de una única vulnerabilidad hace referencia a enlaces rotos, que se explica en la tabla 10.

Ilustración 13: Gráfica Total Vulnerabilidades

Alta = 1, Media = 3, Baja= 3, **Info** 1

4.4.6 Ataques a la aplicación web

Teniendo en cuenta las vulnerabilidades encontradas, procedemos a realizar una prueba de penetración y realizar intentos de intrusión sobre algunas de las debilidades de la página web con el fin de ver qué información se puede obtener.

4.4.7 WordPress

De acuerdo a la vulnerabilidad descrita en la tabla 3, que revela la existencia de un formulario de autenticación del administrador de contenido, se procede a realizar validaciones especializadas adicionales y un ataque de fuerza bruta.

Se ejecuta un escaneo al gestor de contenido WordPress con el cual actualmente está creada la página www.epc.com.co, para esto usamos la herramienta de Kali WPScan, realizando la

configuración de los parámetros adecuados para el escaneo, nos arroja los usuarios administradores de la aplicación y la versión de este.

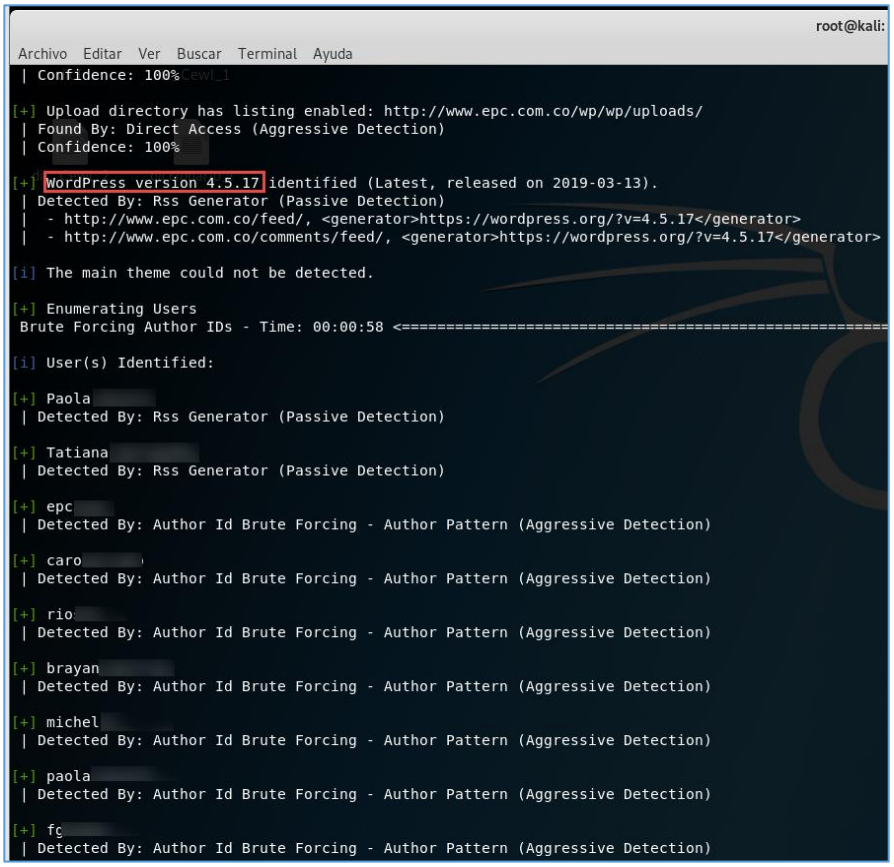


Ilustración 14: Escaneo Gestor de Contenido WordPress

Revisamos la versión del WordPress y al validar que vulnerabilidades tiene asociadas a la misma, encontramos que esta versión es una de las más actuales, 13 de marzo de 2019, por lo cual no encontramos ninguna debilidad conocida. Posterior a esto, ya conociendo los usuarios después de realizar la enumeración de WPScan, se procederá a realizar un ataque de fuerza bruta con el fin de resolver las contraseñas de usuario identificado, optamos por esta opción ya que al probar manualmente el intento de ingreso, nunca se realiza el bloqueo por número de intentos fallidos, de esta forma usamos un diccionario que contiene un numero representativo de contraseñas comunes

usadas por los usuarios (14’350.000 palabras).

Para los ataques de Fuerza bruta usamos WPScan y BurpSuite, sin embargo, no se ha tenido éxito.

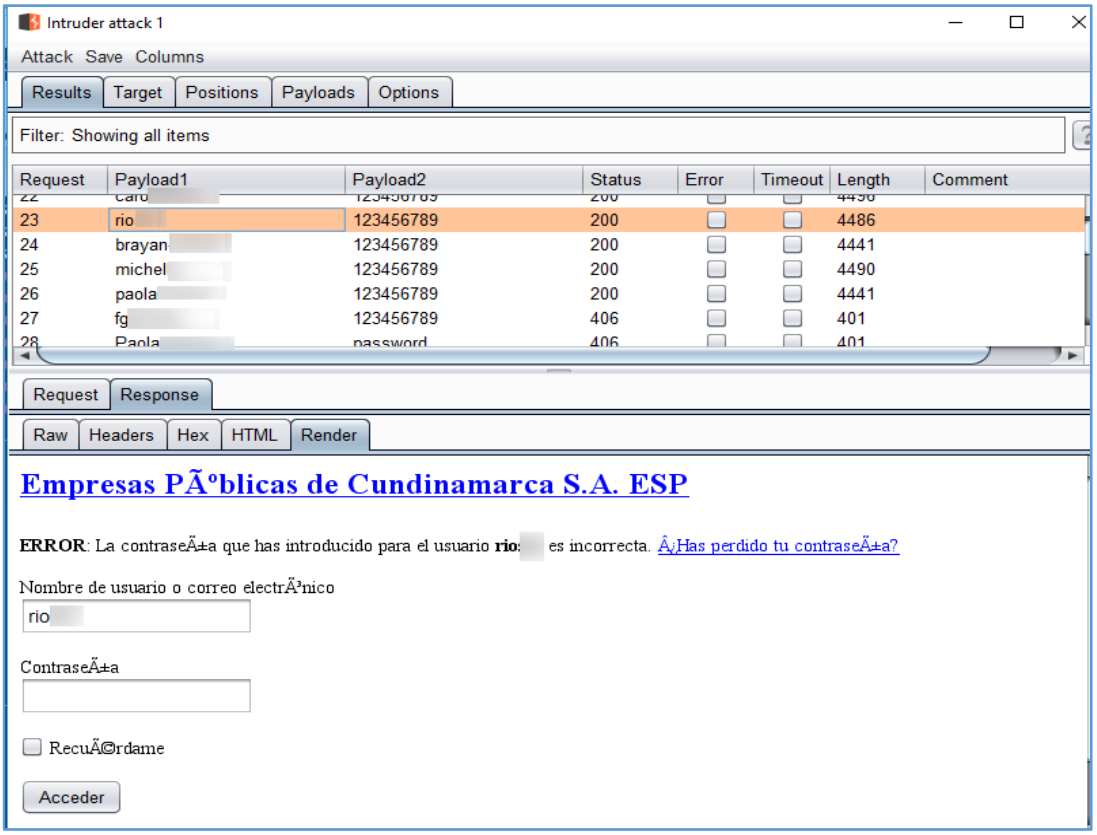


Ilustración 15: *Fuerza Bruta con BurpSuite a www.epc.com.co*

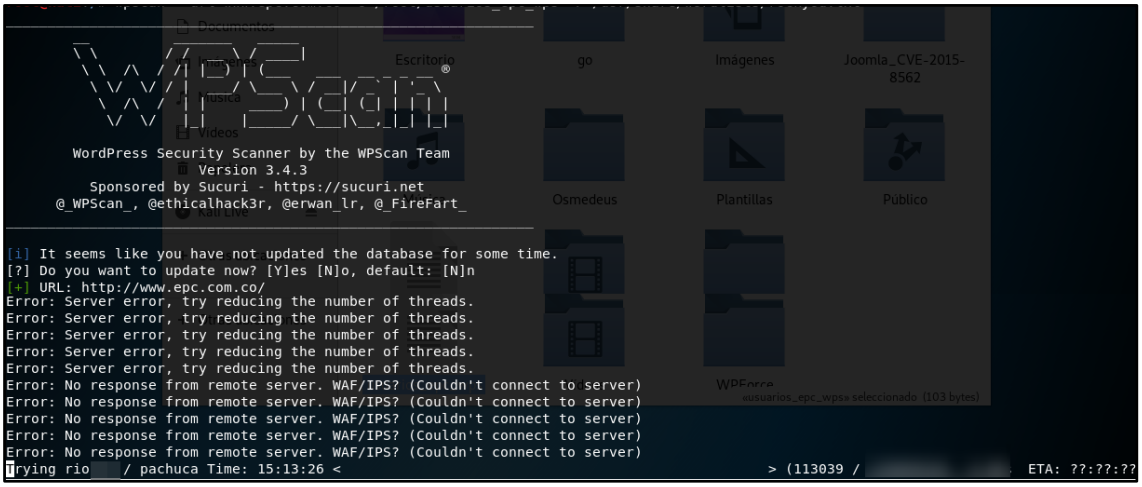


Ilustración 16: *Escaneo con WPScan a www.epc.com.co*

Con lo anterior, vemos que el acceso al administrador de contenidos es vulnerable y que en algún momento se obtendrían las credenciales de acceso para alguno de los usuarios administradores de la aplicación, en contexto, es conveniente que se configure el bloqueo del usuario cuando se generen al menos 5 intentos fallidos, esto ayudaría a corregir los ataques de fuerza bruta. También es buena práctica recomendada la implementación de un Captcha que verifique que el intento de ingreso lo hace un ser humano y no una aplicación o un robot Captcha.

4.4.8 Joomla

De acuerdo a la vulnerabilidad descrita en la tabla 4, en donde se evidencia la existencia de una página de Login al gestor de contenido Joomla se procede con el escaneo al gestor de contenido Joomla con el cual años atrás estaba creada la página www.epc.com.co, para esto usamos la herramienta de Kali JoomScan, realizando la configuración de los parámetros adecuados para el escaneo, nos arroja la versión y las vulnerabilidades que este tiene.

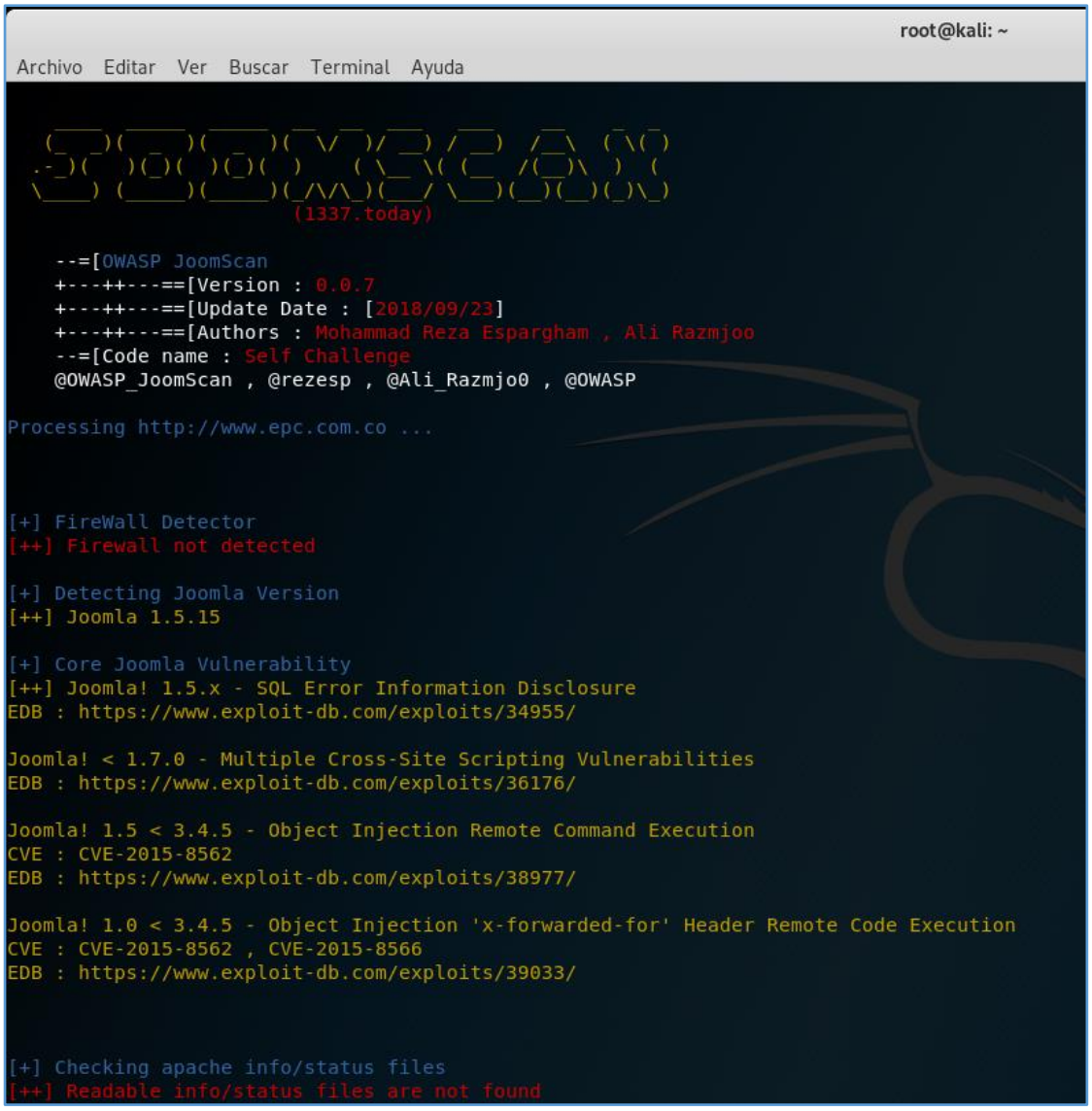


Ilustración 17: Escaneo Gestor de Contenido Joomla

Con la información obtenida luego del escaneo, se observa que la versión del Joomla es la 1.5.15, la cual es una versión de 4 de noviembre de 2009, una versión bastante desactualizada ya que la última versión de este gestor de contenido es 3.9.6 de 7 de mayo de 2019, con lo cual cuenta con vulnerabilidades, una de estas es insertar objetos mediante una conexión remota. Este escaneo también nos permite ver que no se detectó un Firewall, sin embargo, sabemos que el servidor web es un Nginx/1.14.1 y con alta probabilidad puede haber un WAF/IPS que puede generar bloqueos

a los intentos de conexión que se generen.

De acuerdo a lo anterior, existe un exploit que permite la ejecución remota de inyección de objetos php a las cabeceras del Joomla CVE-2015-8562 (NIST, 2015). Procedemos a realizar el ataque con la herramienta Metasploit del Kali, Para esto se realizan las preconfiguraciones necesarias para la ejecución del ataque usando el exploit que se encuentra subrayado en rojo.

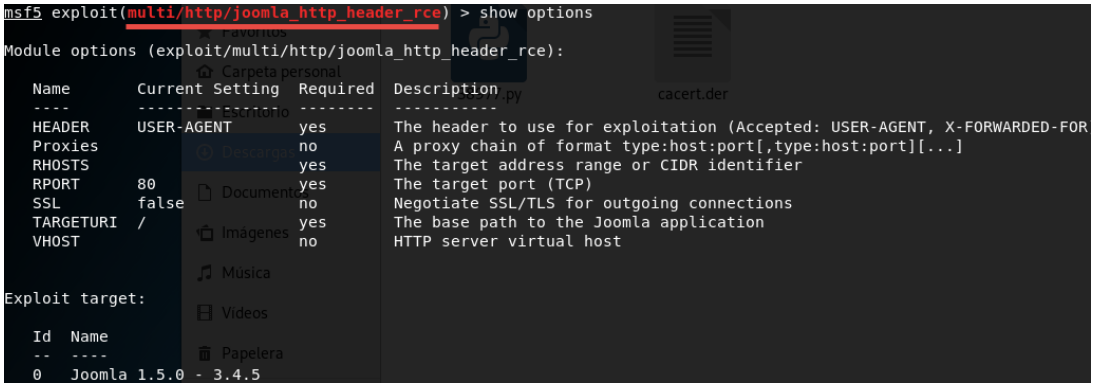


Ilustración 18: Ataque desde el Metasploit al Joomla

El resultado obtenido es una sesión de Meterpreter cerrada (se trata de un intento de ataque de apertura de una sesión remota pero que debido a la no existencia de todas las condiciones técnicas (versiones especificas vulnerables, sistemas de protección habilitados, entre otros.) no es exitoso.), esto debido al servidor NGINX.

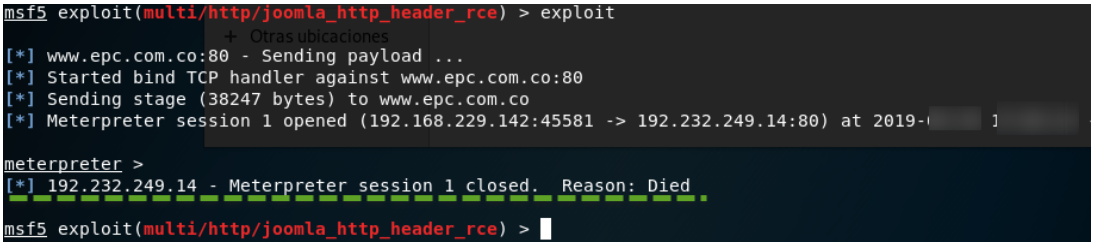


Ilustración 19: Sesión de Meterpeter Cerrada - Joomla

Debido a que este servidor Joomla no contiene toda la información no tiene utilidad representativa hoy día y que se están usando dos gestores de contenido web, se recomienda eliminar Joomla y realizar el cambio definitivo de todo el contenido a WordPress ya que es un administrador de contenido actualizado.

4.4.9 Clickjacking

De acuerdo a la vulnerabilidad descrita en la tabla 1, el atacante podría usar una técnica maliciosa para engañar al usuario que está en la web para que haga clic en algo diferente a lo que el mismo usuario percibe, de manera que se engaña al usuario para que acceda a un sitio malicioso en donde pueden robar su información o descargar algún malware que controle el equipo del usuario.

Ilustración 20: Prueba Online de un ataque Clickjacking

Este tipo de ataques Clickjacking se puede prevenir, el encabezado X-Frame-Options se puede usar para indicar si un navegador debe tener permiso para representar una página en un <frame>o <iframe>. Los sitios pueden usar esto para evitar los ataques de Clickjacking, asegurándose de que su contenido no esté incrustado en otros sitios. Establezca el encabezado X-Frame-Options para todas las respuestas que contengan contenido HTML. Los valores posibles son "DENY", "SAMEORIGIN" o "ALLOW-FROM uri"(OWASP, 2019)

4.4.10 Indexación de Diccionarios

De acuerdo a la vulnerabilidad descrita en la Tabla 6, desde el servidor web es posible listar archivos dentro del algún directorio solicitado, esto puede acarrear que se liste información que el público que no debería ver, uno de los ejemplos más comunes es listar el archivo Robots.txt, el directorio /cgi/ o el directorio /wp, esto permitirá que se vulnera la confidencialidad de la información.

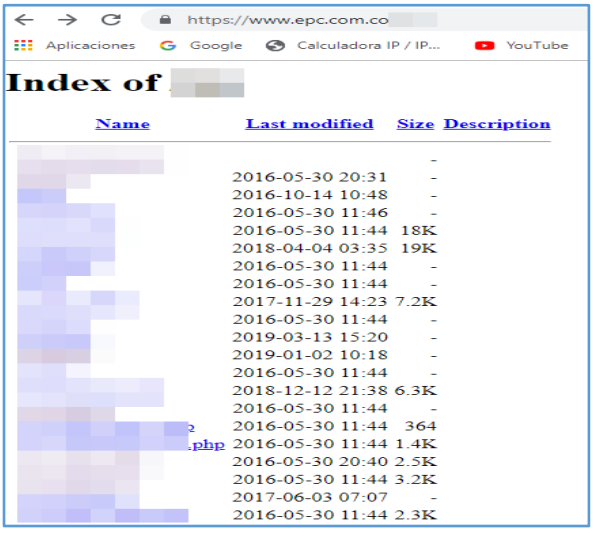


Ilustración 21: Listado Directorio via Web

Asegúrese de que los directorios navegables no filtren información confidencial ni den acceso a recursos confidenciales. Además, use las restricciones de acceso o deshabilite la indexación de directorios. (Tenable-Nessus, 2019)

Se debe restringir el acceso a directorios o archivos importantes y desactivar características tales como los listados automáticos de directorios que podrían exponer archivos privados y proporcionar información que podría ser utilizada por un atacante al formular o realizar un ataque, lo que conlleva a una falla en la confidencialidad e integridad de la información. (CWE, 2018)

4.4.11 Cargue de archivos y suministros de credenciales de usuario en texto claro

Se evidencia en algunos subdominios de la página que los portales de autenticación no viajan de forma cifrada, permitiendo que las credenciales de pudiesen ser capturado, ya sea por un ataque de tipo “man in the middle”, por el robo de una cookie, etc.

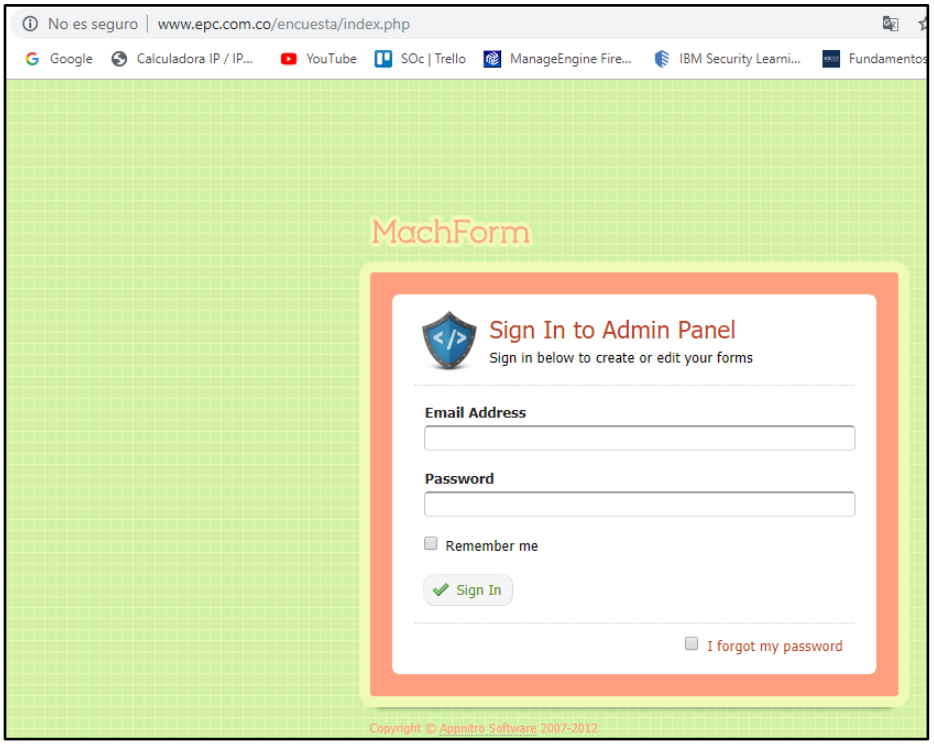


Ilustración 22: Información en texto Claro

Esta página permite a los visitantes subir archivos al servidor. Varias aplicaciones web permiten a los usuarios cargar archivos (como imágenes, imágenes, sonidos, ...). Los archivos cargados pueden suponer un riesgo importante si no se manejan correctamente. Un atacante remoto podría enviar una solicitud POST multipart / form-data con un nombre de archivo o tipo mime especialmente diseñado y ejecutar código arbitrario. (OWASP, 2013)

Teniendo en cuenta lo anterior, para que se realice el adecuado aseguramiento de la información que viaja a través de la página web y de sus portales de autenticación, es necesario que se realice por parte de la empresa la adecuada configuración de certificado digital que actualmente tienen. Se realiza la verificación del certificado ssl en una herramienta online y nos arroja muy bueno resultados, sin embargo, este certificado caducara el 12 de julio de 2019, la idea es renovarlo cuando esto pase y que se mantenga la implementación teniendo en cuenta lo

mencionado líneas atrás, complementariamente, pero no menos importante, es necesario deshabilitar los protocolos TLS 1.0 y TLS 1.1 ya que estos son considerados inseguros.

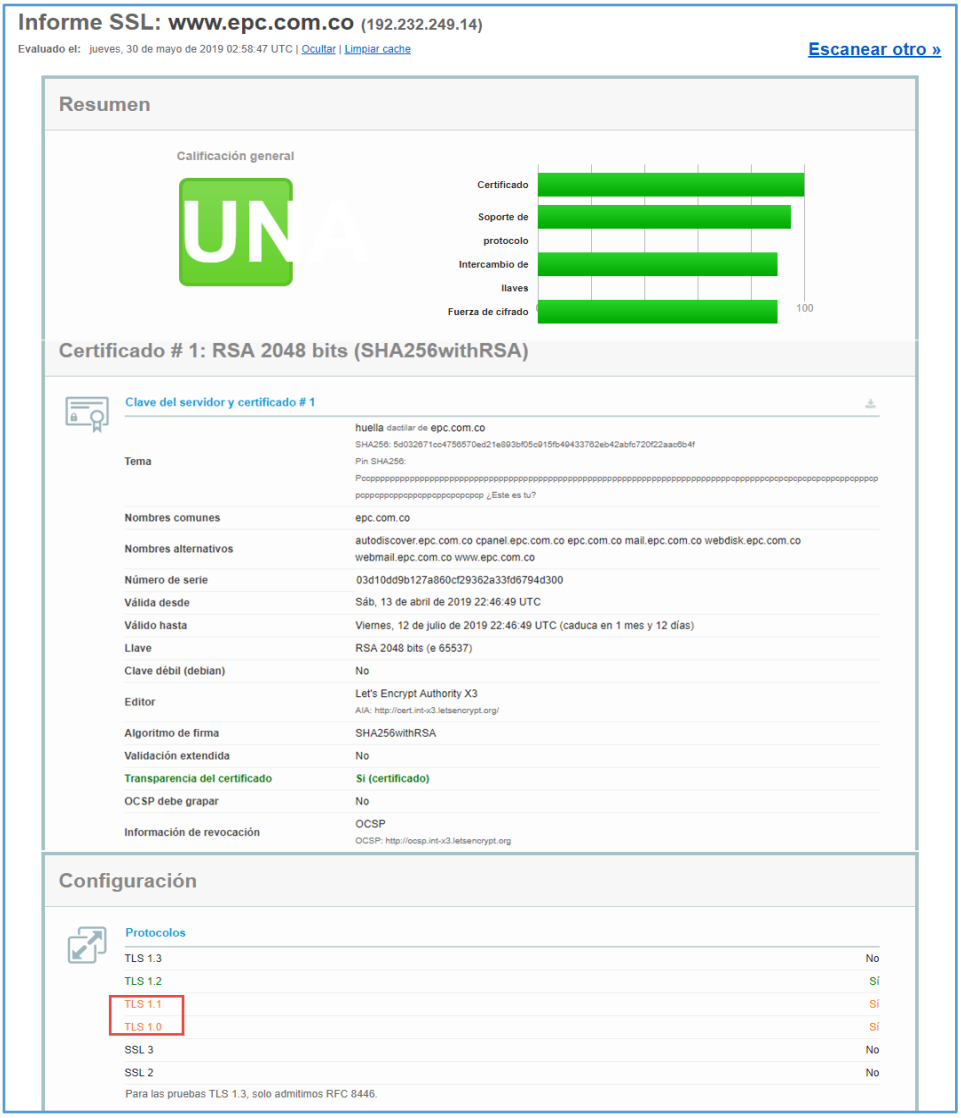


Ilustración 23: Verificacion del Certificado Digital de EPC

4.5 RECONOCIMIENTO DEL OBJETIVO DE INFRAESTRUCTURA (SERVIDORES) DE EMPRESAS PUBLICAS SA ESP Y RESULTADOS DE LAS HERRAMIENTAS UTILIZADAS.

Se utilizó el programa de escaneo de vulnerabilidades Nessus para realizar una serie de pruebas sobre los servidores que se detectaron en la red de la entidad:

En la siguiente figura podemos evidenciar los dos servidores principales de la entidad en los cuales se alojan los sistemas de información:

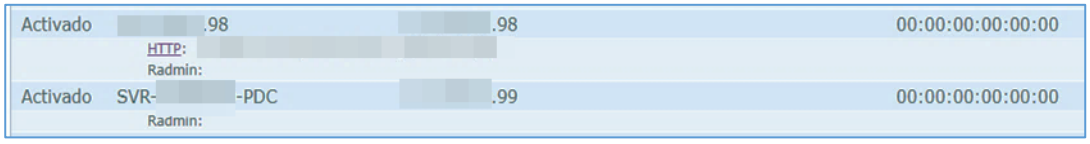


Ilustración 24: Servidores Principales Físicos

En esta figura podemos evidenciar el servidor virtualizado (huésped) que tiene la entidad y sobre el cual se sustenta la base de datos del sistema administrativo y financiero de la entidad:

Ilustración 25: Servidor Huésped Virtualizado

En las siguientes ilustraciones podemos verificar los servidores de almacenamiento en red NAS que tiene la entidad para respaldar la información de los repositorios en las diferentes direcciones y carpetas compartidas:

Ilustración 26: Primer Servidor NAS

Ilustración 27: Segundo Servidor NAS

Ilustración 28: Tercer Servidor NAS

Previo a la realización de la ejecución de la prueba se procedió a realizar la configuración de red inicial en el equipo desde el cual se iban a lazar los procesos de escaneo a los servidores:

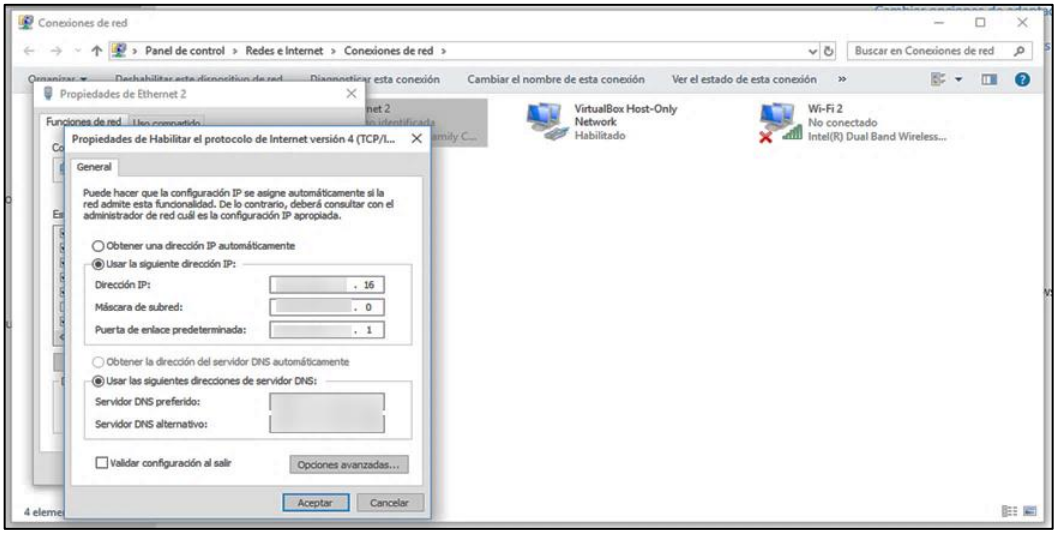


Ilustración 29: Configuración de red en el equipo

Se hace la validación de la última actualización de la herramienta Nessus de tal forma que todos sus componentes estuvieran actualizados:

Ilustración 30: Inicio de Nessus en Kali Linux

Se realiza el inicio de sesión en el programa Nessus para realizar una serie de escaneos avanzados sobre los servidores:

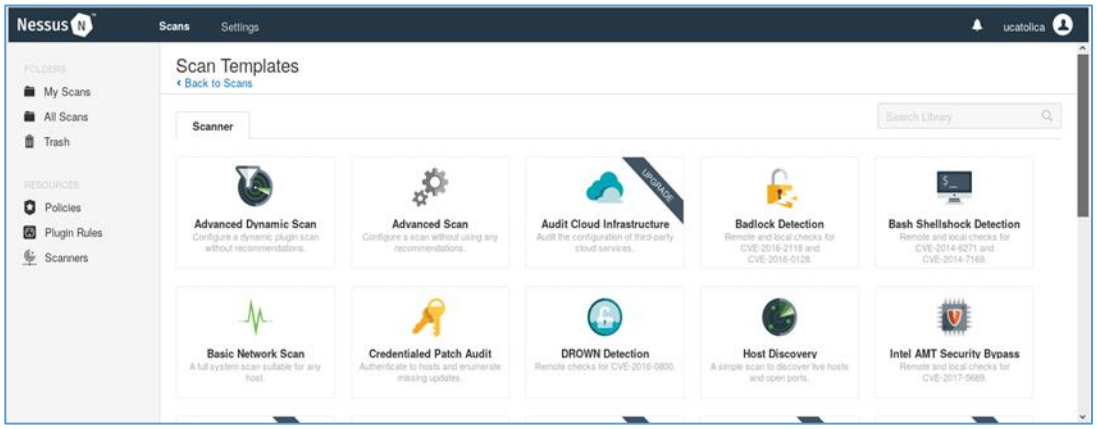


Ilustración 31: Tipo de Escaneo Seleccionado en Nessus

Se procedió a realizar la configuración de la herramienta para la ejecución de cada prueba sobre las IP de la red asignada a cada servidor, de acuerdo a lo descrito inicialmente:

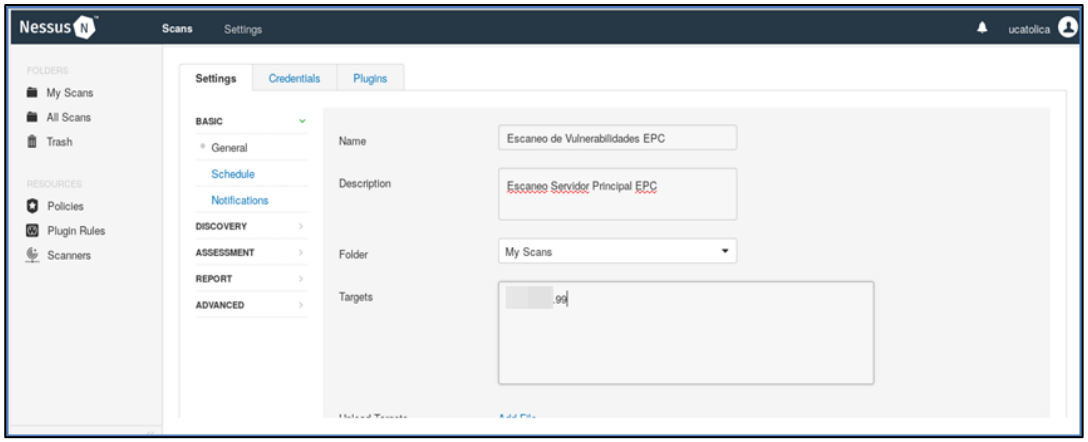


Ilustración 32: Configuración para cada Escaneo

Después de realizar la ejecución de la herramienta Nessus sobre la primera dirección IP identificada como uno de los servidores principales de la entidad que fue el X.X.X.99 y el servidor virtualizado huésped que se encuentra en esta misma maquina con IP X.X.X.191 logrando evidenciar los siguientes resultados:

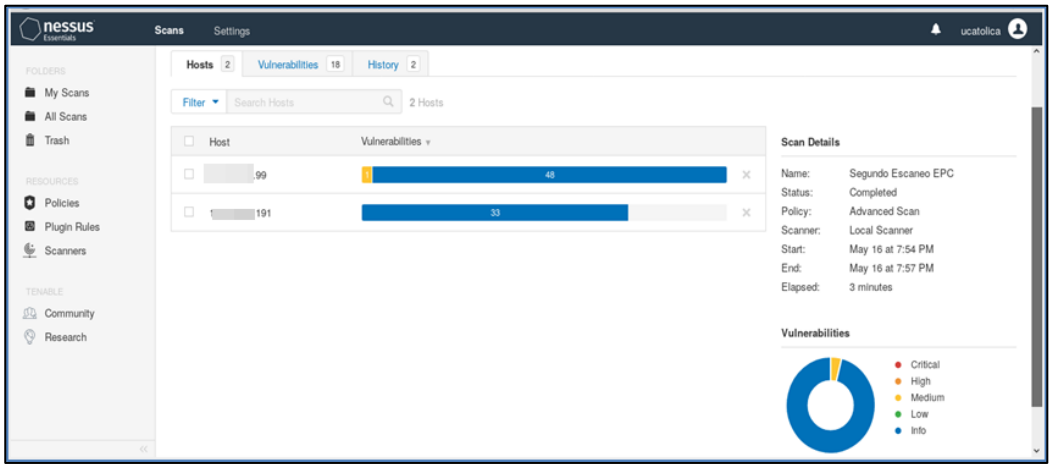


Ilustración 33: Escaneo servidor huésped y anfitrión

Para el servidor físico anfitrión de la virtualización (X.X.X.99) se encuentro un total de 1 vulnerabilidad de tipo medio y 48 tipos Info. Para el servidor virtualizado huésped (X.X.X.191) se encontró un total de 33 tipos Info.

Un segundo escaneo se realizó sobre el segundo servidor físico (anfitrión) principal de la entidad que se identifica con IP X.X.X..98 en la red.

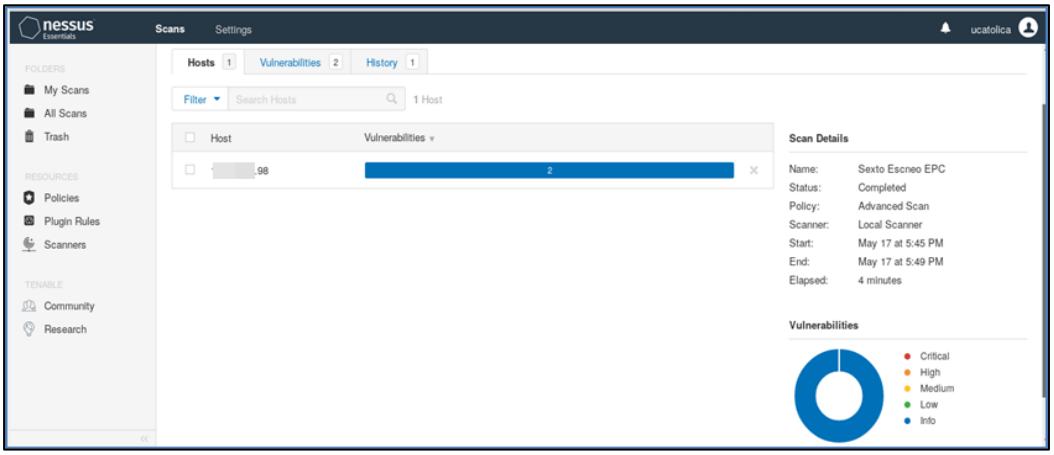


Ilustración 34: Escaneo Segundo servidor físico

En el resultado evidenciamos que únicamente se tiene 3 vulnerabilidades tipo Info. Después del escaneo a los servidores físicos principales y el virtualizado se procede a realizar el escaneo sobre los servidores de red NAS.

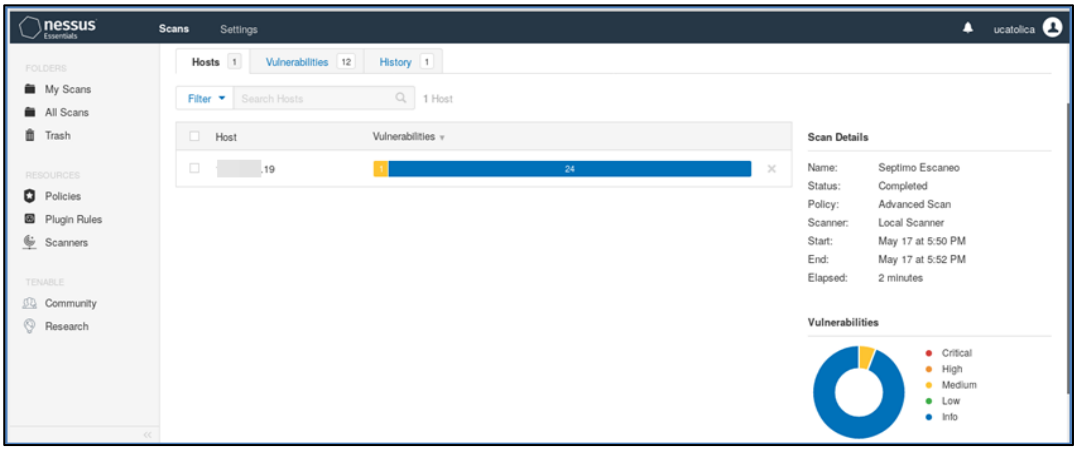


Ilustración 35: Primer Servidor NAS

Para el primer servidor NAS se detecta una vulnerabilidad de categoría media y 24 tipos Info.

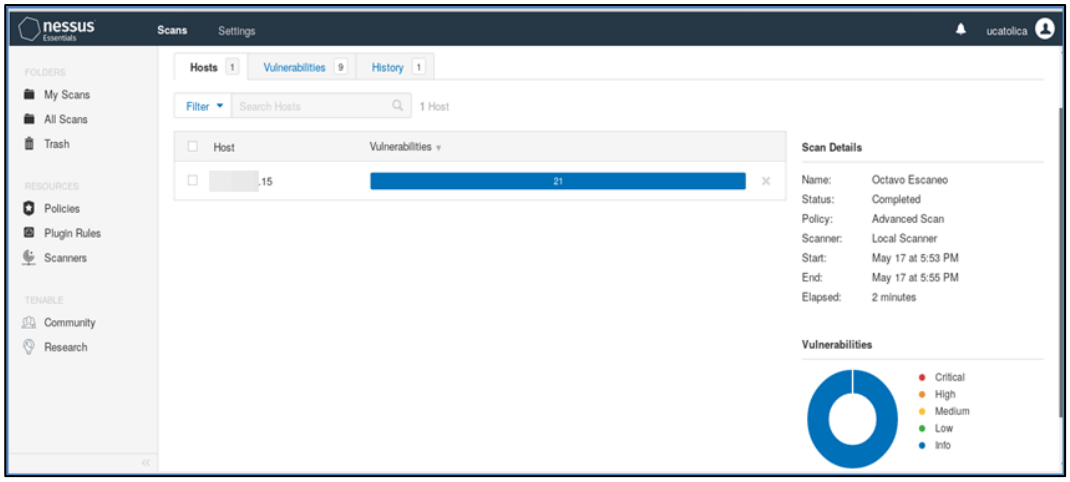


Ilustración 36: Segundo Servidor NAS

Para el segundo servidor NAS se detectan solo 21 vulnerabilidades tipo Info.

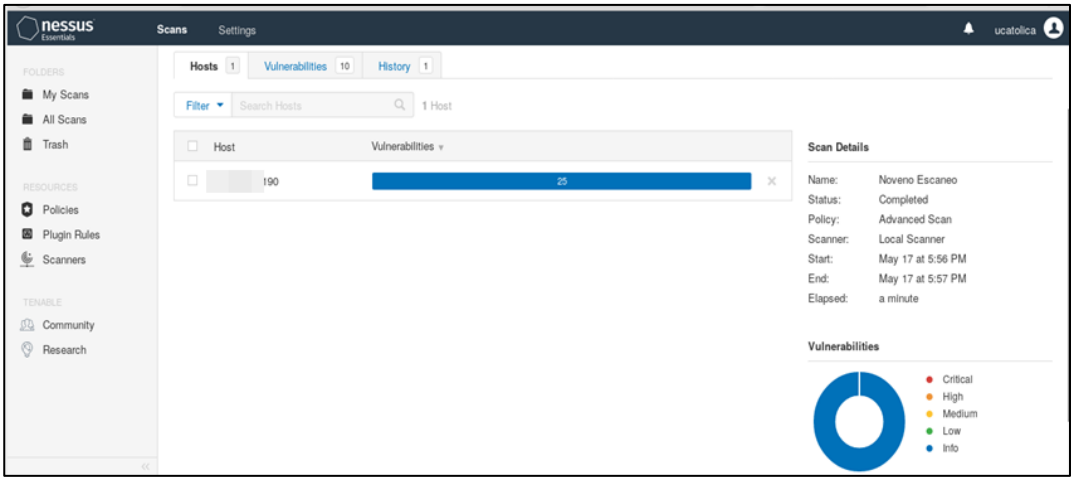


Ilustración 37: Tercer Servidor NAS

Para el tercer servidor NAS se detectan 25 vulnerabilidades tipo Info únicamente.

Para confirmar que Nessus estuviese funcionando correctamente y sus parámetros de configuración asignados según lo requerido, se hizo un análisis de vulnerabilidades sobre un equipo de la red que tiene información sensible del área contable de la organización. Obteniendo

como resultado lo siguiente:

Ilustración 38: Identificación de Equipo de Contabilidad

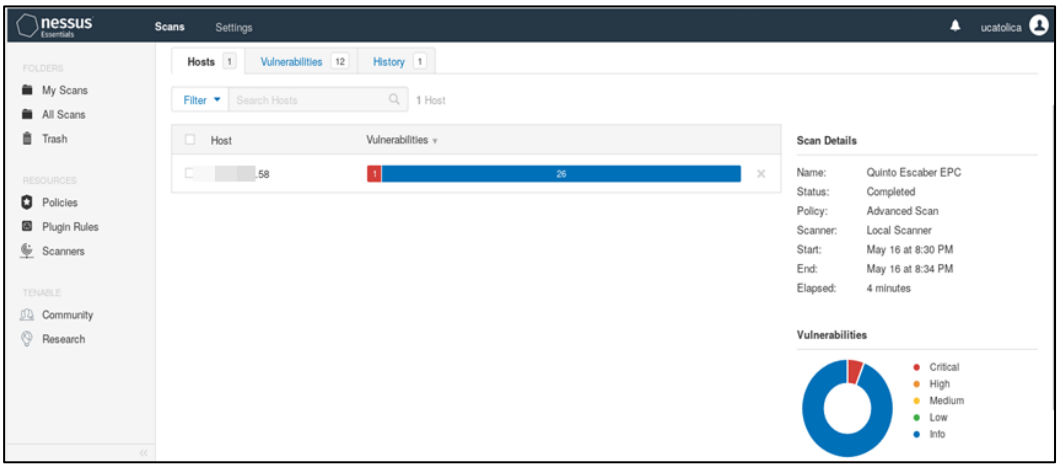


Ilustración 39: Escaneo Equipo en red de Contabilidad usado como repositorio

Como resultado obtenemos una vulnerabilidad de categoría crítica y 26 tipos Info lo que nos permite confirmar que el programa se encuentra bien configurado para la ejecución de la prueba.

Posterior a los escaneos realizados con la herramienta Nessus en cada uno de los servidores de empresas públicas de Cundinamarca podemos determinar que las vulnerabilidades que requieren atención por su importancia son las siguientes:

EQUIPO	VULNERABILIDAD	FACTOR DE RIESGO	DESCRIPCION
Servidor de repositorio Contabilidad	**MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution.**	Alta	Una falla en la forma en que el cliente DNS de Windows instalado procesa las consultas de resolución de nombres de multidifusión local (LinkMNR) para ejecutar código arbitrario en el contexto de la cuenta de NetworkService. En Windows Vista, 2008, 7 y 2008 R2, el problema puede ser explotado de forma remota.
			El servidor DNS remoto responde a las consultas de dominios de terceros que no tienen establecido el bit de

Servidor de aplicaciones principal anfitrión	**DNS Server Cache Snooping Remote Information Disclosure**	Medio	recursión. Esto puede permitir a un atacante remoto determinar qué dominios se han resuelto recientemente a través de este servidor de nombres y, por lo tanto, qué hosts se han visitado recientemente. Si es un servidor DNS interno que no es accesible para las redes externas, los ataques se limitarían a la red interna. Esto puede incluir empleados, consultores y usuarios potenciales en una red de invitado o conexión WiFi si es compatible.
			El host remoto tiene habilitado el reenvío de IP.

Servidor de almacenamiento NAS	**IP Forwarding Enabled**	Media	Un atacante puede explotar esto para enrut ar paquetes a través del host y, posiblemente, evitar algunos servidores de seguridad / enrutadores / filtrado NAC. A menos que el host remoto sea un enrutador, se recomienda que deshabilite el reenvío de IP.

Tabla 10: Vulnerabilidades halladas en el Escaneo Servidores

4.6 MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se alinea con el Marco de Referencia de Arquitectura TI y soporta transversalmente los componentes de la Estrategia Gobierno en Línea – GEL

Mediante la aceptación del MSPI por las Entidades del Estado se busca contribuir al incremento de la transparencia en la Gestión Pública, así como el uso de mejores prácticas de Seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.

El objetivo primordial del MSPI es generar un documento de lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado.

A continuación, detallamos el ciclo de operación del modelo dentro de una organización:

Ilustración 40: *Modelo de Seguridad y Privacidad de la Información*

La realización de una prueba de ethical hacking en empresas públicas de Cundinamarca S.A ESP le permitirá a la entidad cumplir dos de los ítem contemplado en el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACON en lo que hace referencia a la guía marco de referencia de arquitectura empresarial en cuanto a:

4.6.1 Análisis De Vulnerabilidades

- Dominio: Servicios Tecnológicos
- Ámbito: Gestión de la Operación

- Instrumento: Lineamiento – Herramienta de diagnóstico.
- Código: LI.ST.14
- Descripción: La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe implementar el análisis de vulnerabilidades de la infraestructura tecnológica, a través de un plan de pruebas que permita identificar y tratar los riesgos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de TI.

Con la realización del análisis de vulnerabilidades a los servidores de la entidad y la página web podemos dar cumplimiento a uno de los ítem del modelo de seguridad y privacidad de la información en la guía de referencia LI.ST.14 la cual está contemplada a ser realizada por una entidad del estado en la fase de diagnóstico – etapas previas a la implementación.

Con la ejecución de esta prueba la entidad estaría alcanzando una de las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.

- Con la realización de la prueba en la página web y servidor se detectaron vulnerabilidades que comprometen hasta cierto punto algunos de los factores de integridad, disponibilidad o confidencialidad., los cuales se detallan en los informes anexos a la metodología implementada.

4.7 ENTREGA DE RESULTADOS ESPERADOS E IMPACTOS

4.7.1 Aporte de los resultados a la Empresas Públicas de Cundinamarca

Con la prueba de ethical hacking a la página web y servidores de la entidad se logró aportar en el cumplimiento de un ítem del modelo de seguridad y privacidad de la información establecida por MINTIC y de obligatorio cumplimiento para las entidades públicas.

Nos ha permitido dar una visual de que tan vulnerable esta la información almacenada en los servidores de la entidad y la página web.

5 CÓMO SE RESPONDE A LA PREGUNTA DE INVESTIGACIÓN CON LOS RESULTADOS

La respuesta a la pregunta de investigación es que de forma certera la ejecución de un conjunto de pruebas de hacking ético ayudará a EMPRESAS PUBLICAS DE CUNDINAMARCA a adquirir conciencia en relación a la ciberseguridad, también, dio a conocer el actual estado actual de las vulnerabilidades en sus servidores y pagina web, con lo cual los llevará a realizar el aseguramiento de los mismos y ayudará en la reducción del riesgo en la entidad.

Las pruebas realizadas le permiten a Empresas Públicas fortalecer la seguridad de la información en los aspectos en donde se evidenciaron vulnerabilidades o debilidades, además de eso, tendrán un punto de inicio para continuar con aseguramiento de toda la red e infraestructura de información.

Los resultados permiten a Empresas Públicas visualizar lo importante que es la implementación de todas las guías del modelo de seguridad y privacidad de la información MSPI.

6 ESTRATEGIAS DE COMUNICACIÓN Y DIVULGACIÓN

- Divulgación en empresas públicas de Cundinamarca S.A ESP a los responsables y directivos de TI
- Socialización académica en la Universidad Católica de Colombia.
- Publicaciones autorizadas.

7 FORTALEZAS Y DEBILIDADES

7.1 FORTALEZAS

- A nivel web se tienen:
    - Se evidencia que el administrador de contenido WordPress se encuentra actualizado.
- A nivel de servidores se tiene:
    - Se observaron pocas vulnerabilidades, lo que indica que los servidores se encuentran actualizados y que sus instalaciones y configuraciones han contemplado configuraciones de seguridad.

- Los administradores de los servidores tuvieron en cuenta el aseguramiento de estos.

7.2 DEBILIDADES

❖ A nivel web se tienen:

- Se evidencia que cuentan con una versión muy antigua y vulnerable de del administrador de contenido Joomla.
- El certificado digital está próximo a vencer y no está implementado de forma adecuada.

❖ A nivel de servidores se tiene:

- Las dos vulnerabilidades que se detectaron son fallos de configuración que no radicar mayor complejidad en su solución, pero que si pueden generar gran afectación si son atacadas.

8 CONCLUSIONES

- Se evidencio que la entidad lleva un paso lento respecto en la implementación del modelo de seguridad y privacidad de la información MINTIC, sin embargo, en el área de tecnología ha hecho lo posible para realizar un adecuado aseguramiento de la infraestructura, aseguramiento que será reforzado con los resultados y recomendaciones del desarrollo de las pruebas de ethical hacking por parte de los estudiantes de la Universidad Católica.

- Se debe tener en cuenta que hoy en día cada vez los ataques cibernéticos son más sofisticados y que buscan fines lucrativos; la protección de las infraestructuras tecnológicas de las entidades deben evolucionar y buscar la forma de contar con altos estándares de seguridad con el fin de minimizar los riesgos y asegurar los sus activos.

- Por parte del área de tecnología se debe configurar el certificado digital de forma adecuada a la página web de la compañía para que el tráfico vaya cifrado, se debe tener en cuenta que este está próximo a vencer.

- Se debe considerar solo dejar un solo administrador de contenidos para la gestión de la página web ya que tienen dos, uno de estos está muy desactualizado y vulnerables, y tiene un riesgo muy alto de que sea blanco de atacantes.

- Es de resaltar que el administrador de contenidos WordPress se encuentra actualizado.

- En los portales de autenticación se debe implementar un sistema captcha así como el bloqueo después de unos pocos intentos no exitosos de logueo, ya que en este momento un atacante se puede aprovechar de esta debilidad.

- Garantizar la creación de código seguro en aplicaciones y servicios de la organización disminuyendo los incidentes de seguridad.

- Eliminar información obsoleta que se encuentra en la página, ya que estos aparecen como enlaces rotos al ingresar a ellos.

- Realizar una revisión de los recursos visibles dentro de los sitios web.

9 BIBLIOGRAFÍA

Acunetix. (n.d.). Introducción a Acunetix | Acunetix. Retrieved June 2, 2019, from https://www.acunetix.com/support/docs/introduction/

Alycia Mitchell. (2015). WPScan: Encontrando Vulnerabilidades de WordPress. Retrieved June 1, 2019, from https://blog.sucuri.net/espanol/2015/12/usando-wpscan-encontrando-vulnerabilidades-de-wordpress.html

Angarita Pinzón, C., & Guzmán Flórez, C. (2017). *Protocolos para la mitigación de ciberataques en el hogar. Caso de estudio: estratos 3 y 4 de la ciudad de Bogotá*. Retrieved from https://repository.ucatolica.edu.co/handle/10983/15321

CCP-MINTIC. (2016). *Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información*. Retrieved from https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

COLPRENSA. (2018). Colombia, el sexto país con más ciberataques en 2017. Retrieved from https://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174

Congreso de la República de Colombia. Ley 527 de 1999 (1999). Retrieved from https://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

Congreso de la República de Colombia. Ley 1266 de 2008 (2008). Retrieved from https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488&dt=S

Congreso de la República de Colombia. Ley 1712 de 2014 (2014). Retrieved from https://www.mintic.gov.co/portal/604/articles-7147_documento.pdf

E.P.C. (2018). *Plan de Comunicaciones EPC*. Retrieved from http://www.epc.com.co/intranet2012/sig/Servicio al cliente/planes/SAC-Pl002 Plan de Comunicaciones.pdf

El Tiempo, T. (2017). Resultados del estudio Impacto de los incidentes de seguridad digital en Colombia

2017 - Novedades Tecnología - Tecnología - ELTIEMPO.COM. Retrieved from https://www.eltiempo.com/tecnosfera/novedades-tecnologia/resultados-del-estudio-impacto-de-los-incidentes-de-seguridad-digital-en-colombia-2017-137222

EUGENIO DUARTE. (2012). Las 8 Mejores Herramientas de Seguridad y Hacking. Retrieved November 25, 2018, from http://blog.capacityacademy.com/2012/07/11/las-8-mejores-herramientas-de-seguridad-y-hacking/

Fernando Catoira. (2012). Penetration Test, ¿en qué consiste? Retrieved November 25, 2018, from https://www.welivesecurity.com/la-es/2012/07/24/penetration-test-en-que-consiste/

GNU Free Documentation. (2014). The Penetration Testing Execution Standard. Retrieved May 20, 2019, from http://www.pentest-standard.org/index.php/Main_Page

ICONTEC. (2006). *NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001*. Retrieved from http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma. NTC-ISO-IEC 27001.pdf

Iniseg. (2018). ¿Qué es el Hacking ético? Concepto y formación profesional | Ciberseguridad. Retrieved June 3, 2019, from https://www.iniseg.es/blog/ciberseguridad/que-es-el-hacking-etico/

Llanos Ruiz, A. J., & Meneses Ortiz, M. A. (2016). *Diseño de un protocolo para la detección de vulnerabilidades en los principales servidores de la Superintendencia de Puertos y Transporte*. Retrieved from https://repository.ucatolica.edu.co/handle/10983/14013

Miguel Ángel Mendoza. (2015). De la identificación y análisis a la gestión de riesgos de seguridad. Retrieved November 25, 2018, from https://www.welivesecurity.com/la-es/2015/07/16/analisis-gestion-de-riesgos-seguridad/

Ministerio de la Comunicaciones. Decreto 1151 de 2014 (2014). Retrieved from https://www.mintic.gov.co/portal/604/articles-3643_documento.pdf

OWASP-ZAP. (2019). Proyecto Proxy Zed Attack de OWASP - OWASP. Retrieved June 1, 2019, from https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project

OWASP Foundation. (2017). *OWASP Top 10 -2017*. Retrieved from https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

OWASP Joomla. (2018). Categoría: Proyecto de escáner de vulnerabilidad Joomla OWASP - OWASP. Retrieved June 1, 2019, from https://www.owasp.org/index.php/Category:OWASP_Joomla_Vulnerability_Scanner_Project

Revista Dinero. (2017). Sectores más afectados por cibercrimen en Colombia. Retrieved November 25, 2018, from https://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

Revista Dinero. (2018). Incremento de ataques cibernéticos en el 2018. Retrieved from https://www.dinero.com/internacional/articulo/incremento-de-ataques-ciberneticos-en-el-2018/264180

Senado de la República de Colombia. Ley 1273 de 2009 Nivel Nacional, iario Oficial 47.223 de enero 5 de 2009 § (2009). Retrieved from https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

Senado de la República de Colombia. Ley 1581 de 2012 Nivel Nacional, Diario Oficial 48587 de octubre 18 de 2012 § (2012). Retrieved from http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Wikipedia. (2017). Nessus - Wikipedia, la enciclopedia libre. Retrieved June 1, 2019, from https://es.wikipedia.org/wiki/Nessus

Wikipedia. (2019). Nikto (escáner de vulnerabilidad) - Wikipedia. Retrieved May 31, 2019, from https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner)

Wikipedia. (2019). Burp Suite - Wikipedia. Retrieved June 3, 2019, from https://en.wikipedia.org/wiki/Burp_Suite

Wikipedia. (2019). Proyecto Metasploit - Wikipedia. Retrieved June 3, 2019, from https://en.wikipedia.org/wiki/Metasploit_Project

MINTIC. (s.f.). Glosario. Retrieved from https://www.mintic.gov.co/portal/604/w3-propertyvalue-1051.html

Alfonso Lorenzo Perez. (2019). Riesgo, Amenaza y Vulnerabilidad (ISO 27001) - EQ2B Consulting. Retrieved June 3, 2019, from https://eq2b.com/riesgo-amenaza-y-vulnerabilidad-iso-27001/